

2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

AD-A236 835



DTIC
ELECTE
JUN 12 1991
S B D

THESIS

LOCAL AREA NETWORKING HANDBOOK

by

Patricia A. O'Hara

June 1990

Thesis Advisor:

Myung W. Suh

Approved for public release; distribution is unlimited

91-01907



91 6 11 185

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION/AVAILABILITY OF REPORT		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE			Approved for public release; distribution is unlimited		
4. PERFORMING ORGANIZATION REPORT NUMBER(S)			5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School		6b. OFFICE SYMBOL (If applicable) AS	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School		
6c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000			7b. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
8c. ADDRESS (City, State, and ZIP Code)			10. SOURCE OF FUNDING NUMBERS		
			PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.
					WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) LOCAL AREA NETWORKING HANDBOOK					
12. PERSONAL AUTHOR(S) O'HARA, Patricia A.					
13a. TYPE OF REPORT Master's Thesis		13b. TIME COVERED FROM _____ TO _____		14. DATE OF REPORT (Year, Month, Day) 1990 June	
15. PAGE COUNT 92					
16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	Local Area Network; Local Area Networking; LAN		
19. ABSTRACT (Continue on reverse if necessary and identify by block number) This thesis provides Navy shore based commands with sufficient information on local area networking to 1) decide if they need a LAN, 2) determine what their networking requirements are, and 3) select a LAN that satisfies their requirements. LAN topologies, transmission media, and medium access methods are discussed. In addition, the OSI reference model for computer networking and the IEEE 802 LAN standards are explained in detail. A method for conducting a LAN requirements assessment is discussed, followed by a strategy for selecting a local area network.					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL SUH, Myung W.			22b. TELEPHONE (Include Area Code) 408-646-2637		22c. OFFICE SYMBOL AS/Su

Approved for public release; distribution is unlimited

Local Area Networking Handbook

by

Patricia A. O'Hara
Lieutenant Commander, United States Navy
AB, Belmont Abbey College, 1978


Submitted in partial fulfillment of the
requirements of degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS
SYSTEMS MANAGEMENT


from the

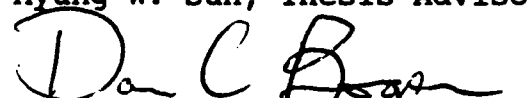
NAVAL POSTGRADUATE SCHOOL
June 1990

Author:


Patricia A. O'Hara

Approved by:


Myung W. Suh, Thesis Advisor


Dan C. Boger, Second Reader


David R. Whipple, Chairman
Administrative Sciences Department

ABSTRACT

This thesis provides Navy shore based commands with sufficient information on local area networking to 1) decide if they need a LAN, 2) determine what their networking requirements are, and 3) select a LAN that satisfies their requirements. LAN topologies, transmission media, and medium access methods are described. In addition, the OSI reference model for computer networking and the IEEE 802 LAN standards are explained in detail. A method for conducting a LAN requirements assessment is discussed, followed by a strategy for selecting a local area network.

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	



TABLE OF CONTENTS

I. INTRODUCTION.....	1
A. PURPOSE.....	1
B. OVERVIEW OF LOCAL NETWORKS.....	2
C. LOCAL AREA NETWORKS.....	4
1. Network Topology.....	7
a. Star Topology.....	7
b. Ring Topology.....	8
c. Bus Topology.....	9
d. Tree Topology.....	11
2. Medium Access Method.....	11
3. Transmission Media.....	12
a. Twisted Pair.....	12
b. Coaxial Cable.....	13
c. Fiber Optic.....	15
d. Summary.....	17
II. COMPUTER NETWORKING STANDARDS.....	19
A. INTRODUCTION.....	19
B. INTERNATIONAL STANDARDS ORGANIZATION (ISO) NETWORK MODEL.....	19
1. Physical Layer (Layer 1).....	23
2. Data Link Layer (Layer 2).....	25
3. Network Layer (Layer 3).....	27
4. Transport Layer (Layer 4).....	29
5. Session Layer (Layer 5).....	30
6. Presentation Layer (Layer 6).....	31

7.	Application Layer (Layer 7).....	31
C.	IEEE 802 STANDARDS.....	32
1.	IEEE 802.2 Logical Link Control Standard (LLC)...	34
2.	IEEE 802.3 CSMA/CD.....	42
3.	IEEE 802.4 TOKEN BUS.....	43
4.	IEEE 802.5 TOKEN RING.....	48
D.	DEPARTMENT OF DEFENSE PROTOCOL STANDARDS.....	51
III.	LAN REQUIREMENT DETERMINATION.....	53
A.	INTRODUCTION.....	53
B.	LAN SERVICES.....	53
C.	ORGANIZATIONAL REQUIREMENTS.....	54
D.	LAN ALTERNATIVES.....	57
IV.	STRATEGY FOR SELECTING A LOCAL AREA NETWORK.....	59
A.	INTRODUCTION.....	59
B.	PERFORMANCE COMPARISON BETWEEN CSMA/CD, TOKEN BUS, AND TOKEN RING.....	59
C.	TOKEN RING VERSUS ETHERNET.....	64
D.	LAN COMPONENTS.....	65
1.	Lan Servers.....	66
2.	Network Control.....	67
3.	Pathways versus Names.....	68
4.	Integration of Services.....	69
E.	LAN PRODUCTS.....	70
F.	WHERE TO GO FOR HELP.....	74
V.	CONCLUSION.....	75
	APPENDIX A:LOCAL AREA NETWORK REQUIREMENTS QUESTIONNAIRE.....	78
	APPENDIX B:NARDAC AND NAVDAF LOCATIONS.....	82

REFERENCES.....83

DISTRIBUTION LIST.....85

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to provide information that will be of value to a Navy shore-based command contemplating the installation of a local area network (LAN) to link their personal computers together. It will provide a reference tool for an action officer who has been tasked with evaluating the feasibility of installing a LAN and will assist in answering the following questions:

1. What is a LAN and what are the current LAN standards?
2. What factors should be considered in determining if an organization would benefit from a LAN?
3. What is a good strategy to follow in selecting a LAN?
4. What other factors need to be considered?

This thesis assumes that a shore-based command already has a number of personal computers and peripherals, and is contemplating the value of linking them together to form a LAN. It also assumes that these personal computers are IBM compatibles (i.e., Zenith-151, Z-158, Z-248, Z-286, Z-386, IBM PC, PC-XT, PC/AT, Compaq Deskpro 286 and Deskpro 386), although most of the information presented is applicable to all types of personal computers.

B. OVERVIEW OF LOCAL NETWORKS

A local network is a communications network of terminals, hosts, and other devices that are located within a small geographic area (normally less than 50 kilometers (km)) for the purpose of sharing resources and exchanging voice, video, graphics or digital data. The nature of a local network falls somewhere between a multiprocessor system and a long-haul data network and is determined primarily by two factors: topology and medium access control protocol. [Ref. 1:p. 39]

The major characteristics of a local network are:

1. High data rates (0.1-100 Mbps).
2. Short distances (0.1-50 km).
3. Low error rate (10^{-9} - 10^{-11}).
4. Interconnection of otherwise independent devices.
5. Inexpensive transmission media and devices are used to interface to the network.
6. Every device has the potential to communicate with every other device on the network. [Ref. 2:p. 4]

A number of potential benefits motivate the procurement of a local network. One of the most important is the support a local network provides for system expansion and evolution. In a well-designed network, additions and replacements can be made with little impact on the other devices on the network. Hence, a system can evolve cheaply and gradually, rather than going through a few major upgrades or replacements. An equally important benefit is the high availability afforded by the local network. Critical resources can be replicated with no interconnection problems. Functions can be shifted from failed processors to alternate processors with little trouble. There is a wide range of other benefits as well, including

sharing of expensive resources, integration of office automation and data processing, and flexibility of equipment location. [Ref. 1:p. 40]

There are three major types of local networks: local area network (LAN), high-speed local network (HSLN), and digital switch/digital private branch exchange (PBX). The local area network (LAN) is generally used to describe a general-purpose local network that can support a wide variety of devices such as mini-computers, mainframes, terminals, and other peripherals. The high-speed local network (HSLN) is designed to provide high throughput between expensive, high-speed devices, such as mainframe and mass storage devices, for such uses as file and bulk data transfer, automatic backup, and load leveling. In contrast to the LAN and HSLN, which use packet transmission, the digital switch and PBX use circuit switching. The PBX is well suited to voice traffic and to both terminal-to-terminal and terminal-to-host data traffic. Table 1 summarizes the general representative characteristics of each type of local network.

The local area network is the most widely used local network in military applications because it can easily be adapted to a variety of devices and a mix of data traffic types; therefore, this thesis will concentrate on LAN technology.

TABLE 1
TYPES OF LOCAL NETWORKS
[Ref. 3:p. 334]

	Local Area Network	High-Speed Local Network	Digital Private Branch Exchange
Transmission medium	Twisted pair, coax (both), fiber	CATV coax, fiber	Twisted pair
Topology	Bus, tree, ring	Bus, ring	Star
Transmission speed	1-20 Mbps	50-100 Mbps	9.6-64 kbps
Maximum distance	25km	1km, 25 km	1km
Switching technique	Packet	Packet	Circuit
Number of devices supported	100's-1000's	10's, 1000's	100's-1000's
Attachment cost	\$500-\$5000	\$40k-\$50k	\$250-\$1000

C. LOCAL AREA NETWORKS

Due to the evolutionary nature of LAN technology, there is no consistent definition of a LAN. However, most experts agree that LANs should have three main characteristics, and they will serve for purposes of this thesis:

1. Utilization of some type of switching technology,
2. Locality restricted to a few miles or in the same building, and
3. Proprietorship by a single organization (privately owned).

[Ref. 4:p. 7]

Local area networking is a relatively new concept, the development of the earliest networks having begun in the early 1970's. It is worthwhile to explore some of the advancements which lead to the germination of LANS.

It can be argued that there were two developments that made LANs possible -- packet switching and microchip technology. Each will be covered separately.

Packet switching is a dynamic-allocation technique (as opposed to pre-allocation) whereby bandwidth is allocated only when a block of data is ready to be sent, and only enough for that one block of data to travel over one network link at a time. [Ref 5:p. 43] Integral to packet switching is the packet itself, which is defined as:

A group of bits that includes both control and data information that is transmitted as a unit. The control information that is carried in the packet provides for such functions as addressing, sequencing, flow control and error detection/correction. [Ref. 6:p. 48]

The concept of packet switching with computers dates back to the early 1960's, in response to a need to communicate data to and from computers. The first operational packet switching system was ARPANET, which connected universities and research institutions by using minicomputers at each site as the packet switch and interface device, interconnected by 56 kbps lines. Four nodes of this net were operational by December 1969. [Ref. 5:p. 44]

In early 1971, the Aloha packet radio network was developed. This system was the first to employ radio instead of point-to-point wires for its computer communications, and it employed packet switching. The system was developed by the University of Hawaii to provide communications between the main computer center on Oahu and the other campuses in the university system (seven campuses on four islands). The Aloha network used radio channels to transmit messages without checking whether or not the channel was already in use. If a

collision took place the sender would retransmit his message after a random interval.

The concepts of packets and packet switching were effectively demonstrated by the ARPA and Aloha networks, and both are used in LANs today.

The tremendous developments in microchip technology, including the significantly improved price to performance ratio, has resulted in increased computing power in smaller machines for less money. By the early 1980's, microprocessors could already be built on a single chip to be as powerful as the room-sized IBM machines of the late 1960's. [Ref. 7:p. 170] The personal computer is a direct result of this technology, as are the local area networks that tie them together.

It is interesting to note that the first computer networks (i.e., the ARPA and ALOHA networks) were really wide-area networks, in the sense that they covered a large geographic area. Ethernet, the first "local area network" developed in the early 1970's, was used to connect workstations and peripherals to a mainframe computer. The personal computer LAN (PC LAN), which is the topic of this thesis, did not come about until much later.

Once an organization has decided that it has a valid requirement for a local area network, there are several important and inter-related decisions which will need to be made concerning network topology, medium access method, and

transmission media. The purpose of this section is to provide an introduction to these considerations, which will provide a basis for more detailed discussion in Chapter Two.

1. Network Topology

Network topology determines the manner in which the switching nodes, user devices, and transmission lines are interconnected. There are four major LAN topologies, with most actual networks designed to use a mixture of topology types. The following sections will describe the star, ring, bus, and tree topologies, illustrated in Figure 1.

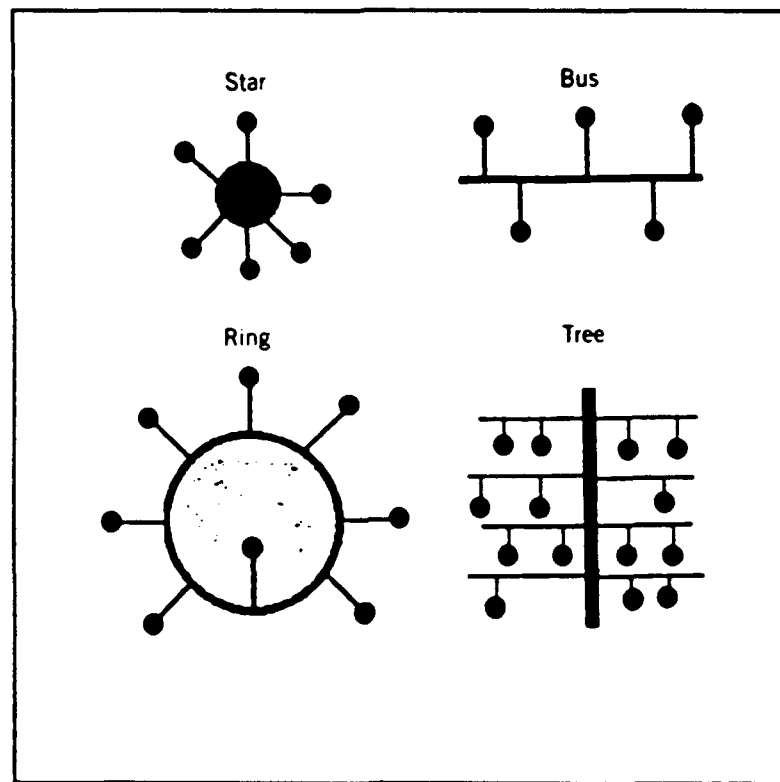


Figure 1. Network Topologies [Ref. 8:p. 35]

a. Star Topology

In the star topology, each network consists of a central node or hub, through which all traffic must pass, and

network nodes, connected to the hub by separate lines, which transmit and receive traffic. [Ref. 9:p. 10] When messages are sent between network nodes, the transmitting node makes the request to the central node, which in turn establishes a path to the receiving node.

The star configuration is the oldest and least reliable type of network configuration and has two major drawbacks -- 1) it requires a great deal of cable since each network node must be connected to the hub, and 2) failure of the hub brings down the whole system. [Ref. 8:p. 35]

"The star is normally not used in LANs except where the physical wiring of the transmission medium bridges all conductors together at a common point creating the electrical equivalent of a bus." [Ref. 10:p. 504]

Since this configuration is the least effective and is therefore not widely utilized, it will not be discussed any further.

b. Ring Topology

A ring network consists of nodes with connections only to one other node on each side, such that a complete circle is obtained. A ring network differs from a star network in that there is no central hub, or switch, which controls the network. The ring design attempts to avoid the potential reliability problems with the central node of a star. Nodes are able to transmit or receive data in either direction on the ring with full duplex links, but data must pass through all nodes between the sender and the receiver

with the possibility of a shorter path in one direction or the other. Unidirectional ring topologies are more common.

Each node on the ring is associated with a repeater. Information passing between nodes on the ring is easy because there is only one path into and out of a repeater. A message is continuously regenerated as it passes through each repeater and will continue to circulate unless removed by the addressed node or by the transmitting node, depending upon the implementation and protocol. Because of the data transmission rates used with both ring and bus topologies (typically from 1 - 10 Mbps), they are best suited for interconnecting networks with a small number of nodes operating at high speeds over short distances. [Ref. 1:p. 314]

c. Bus Topology

A bus network has nodes connected to the same transmission medium. A signal transmitted by a node will propagate in both directions along the bus. Normally a single network cable is routed through those locations (offices) that have data terminal equipment (DTE) to be connected to the network, and a physical connection (tap) is made to the cable to allow the user DTE to gain access to the network services supported. The bus is typically time or frequency multiplexed, allowing nodes to transmit information in short-duration, high-speed bursts. There are basically two types of

buses, baseband and broadband, both of which will be discussed separately:

- Baseband: In the baseband bus topology, only one node can transmit at a given time. If two or more nodes try to transmit at the same time, the information is damaged and must be retransmitted. Different protocols are used to determine the way in which time slots are allocated.
- Broadband: A broadband network uses technology similar to the cable television (CATV) system. A broadband network can carry many different signals at the same time by use of frequency-division multiplexing (FDM). Typically, in broadband networks, a headend is placed at one end of the bus. Its job is to convert frequencies used for transmitting into frequencies used for receiving.

With broadband networks, a great many simultaneous, independent communications paths are possible in real time, and it is not necessary to depend on an access protocol to mediate between numerous interfaces vying for time on the bus. An FDM network, like conventional communications media, simply supplies a transparent communications medium. Any conventional circuit configuration (i.e., point-to-point or multipoint) may be implemented using broadband cable by substituting RF modems for the conventional modems or line drivers. Then control may be imposed through conventional communications link protocols (such as binary synchronous communications (BSC) and synchronous data link control (SDLC)) enacted by the communicating devices themselves. [Ref. 11:p. 33]

In a typical broadband bus configuration using FDM, channels are allocated dynamically, using frequency agile RF modems, rather than statically. The network may use a

contention channel for channel requests and demand allocated channels for traffic.

d. Tree Topology

The tree is an expanded version of the bus topology, and is often used in LANs employing cable television technology. It is electrically identical to the bus, except that the branches of the tree must be connected only through properly designed impedance-matching devices.

2. Medium Access Method

In a broadcast network such as a local area network, no more than one station can transmit data on a shared medium at a time because all stations share a common cable. Therefore, a medium access control (MAC) scheme is required to determine which station may transmit next without collision. The key parameters in any medium access control technique are where and how. "Where" refers to whether control is exercised in a centralized or decentralized fashion. In a centralized scheme, a controller will grant access to the network station who must wait for permission to transmit. In a decentralized network, the stations collectively perform a MAC function to dynamically determine the order in which stations transmit. The second parameter, "how", is constrained by the topology and is a tradeoff among competing factors: cost, performance, and complexity. [Ref. 3:pp. 208-209]

There are two different types of protocols that have evolved for access to local area networks. The first involves

carrier-sensing; that is, a station wishing to transmit will listen to the transmission medium and will transmit when it is clear. If two stations attempt to transmit simultaneously their packets will collide, so there must be a mechanism to allow for collision detection and retransmission of effected packets. The second method involves some form of token passing. In a token passing network, only the station with the token can transmit. When transmission is complete, it will free the token for use by the next station designated to receive it. There are advantages and disadvantages to both of these methods, and they will be covered in detail in Chapter Two.

3. Transmission Media

Although theoretically speaking, any transmission media could be used in a LAN, in practicality three types are used; twisted pair wire, coaxial cable, and fiber optic cable. The purpose of this section is to provide basic information on each of these alternatives.

a. Twisted Pair

Twisted pair wire is best described as two insulated, thin copper wires twisted in a regular spiral fashion. The twisting of the wires serves to reduce electromagnetic interference between the pairs. The wire pair provides a single communications link. The thickness of the wire pair is measured in gauges (0.016" - 0.036"). For example, 26 gauge is thin and light, whereas 19 gauge is

thicker and heavier. The most extensive use of twisted pair wire is in the telephone system, where it provides the link between the individual telephone instrument and the local telephone exchange. Twisted pair also has applications for local area networking.

Twisted pair has the following advantages and disadvantages:

- Advantages: Twisted pair is characterized by low cost and easy implementation. Installation of twisted pair is simple because of its small size and the flexibility of the cable.
- Disadvantages: In LAN applications, twisted pair can be used for only short distances (around 1 km), the data rate is slower than coaxial cable or optical fiber (around 1 Mbps for unshielded twisted pair), and fewer devices can be supported. Twisted pair is also more susceptible to interference, outside electromagnetic problems, and interception.

b. Coaxial Cable

Coaxial cable is similar to twisted pair in that it has two conductors, but it is constructed differently as shown in Figure 2.

There are two conductors -- inner and outer. The inner conductor may be solid or stranded, with the outer conductor either solid or braided. The inner and outer conductors are separated by either an insulating spacer or

solid dielectric, and the outer conductor is covered by a durable outermost jacket or shield. The primary uses of coaxial cable are long-distance telephone and television, cable television, and local area networking. [Ref 3:p. 50]

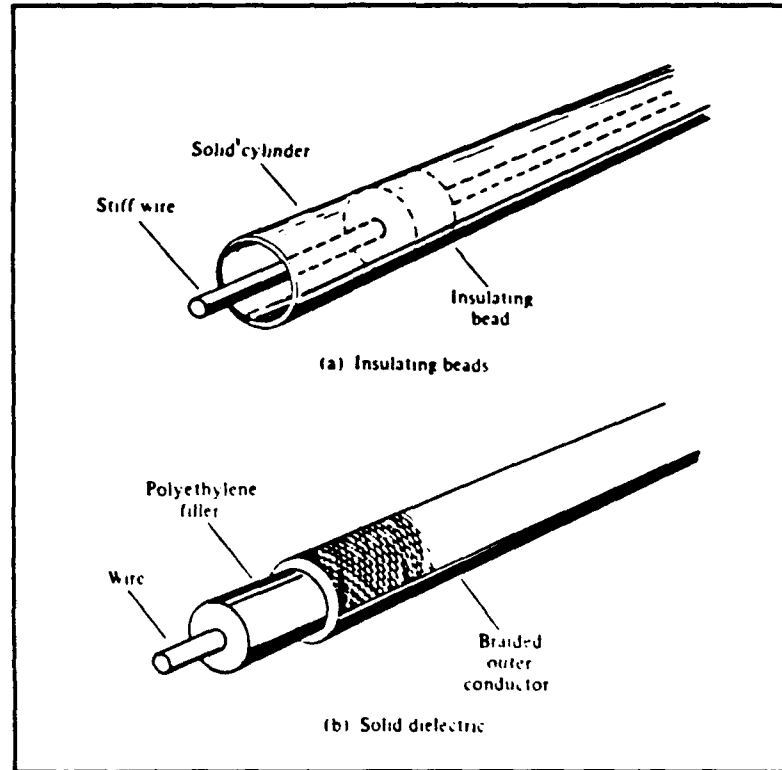


Figure 2. Coaxial Cable Construction
[Ref 3:p. 51]

Coaxial cable has the following advantages and disadvantages:

- Advantages: In comparison with twisted pair, coaxial cable can carry higher frequencies, support greater data rates, and travel greater distances. Coaxial cable can also support both baseband and broadband LANs.

- Disadvantages: Coaxial cable is less flexible than twisted pair, and can cost three to five times as much. Nevertheless, it is the media of choice for most LAN applications.

c. Fiber Optic

There are three different materials which can be used to construct optical fibers -- ultrapure fused silica, which is the most difficult to manufacture and therefore most expensive, multicomponent glass, and plastic. Most LANs which use optical fiber use the multicomponent glass variety, although at least one (Fiberstar) uses the plastic fiber.

[Ref. 12:p. S3]

All optical fibers are composed of three sections:

- core - innermost section, consisting of thin strands of glass or plastic,
- cladding - glass or plastic coating of each core fiber which had different optical properties than the core, and,
- jacket - protects the fiber against the environment and is normally composed of plastic or similar material.

Figure 3 shows a basic optical fiber communication link.

There are three types of fiber, multimode step index, multimode graded index, and single mode step index. The single mode fiber has applications in long-haul communications, but is generally not used in LANs due to the

expensive electronics and connectors which are required. Multimode fibers are most often found in LANs today. [Ref. 14:p. 51]

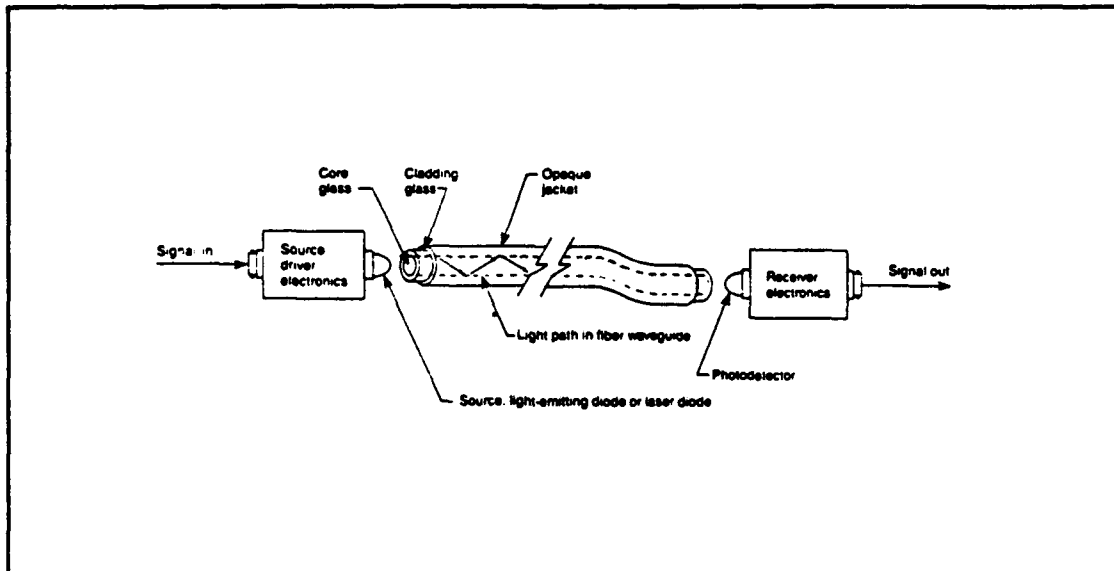


Figure 3. Basic Optical Fiber Communication Link
[Ref. 13:p.154]

Optical fiber has the following advantages and disadvantages:

- Advantages. It is thin, light, and flexible. The cost of optical fiber is decreasing. In addition, optical fiber offers the following:

1. Speed: 100 megabits per second or more.
 2. Immune to electrical noise: You can run cabling right under an electrical motor.
 3. Low error rate: Less than one bit per billion.
 4. Durable: Can't corrode and can be run under water.
 5. Good security: Harder to tap than copper wire.
- [Ref. 12:p. 53]

In short optical fiber has many inherent advantages over twisted pair wire and coaxial cable and will

probably be the transmission media of choice for LANs in the future.

- Disadvantages. The overwhelming argument against the use of fiber optic cable in LANs at present is the lack of approved standards. FDDI, a standard for a fiber optic network incorporating a physical star and a logical ring, is still years down the road. There are products available (approximately 160 vendors are selling fiber optic LAN products), but there is a serious lack of interoperability between vendors. For a command that needs a LAN now and can operate within the bandwidth constraints imposed by twisted pair wire or coaxial cable, the best advice is to use them. It will be several more years before fiber optic will have matured to the point of becoming the preferred choice for PC LANs.

d. Summary

Table 2 provides a summary comparison of twisted pair wire, coaxial cable, and fiber optic cable.

TABLE 2
SUMMARY OF CHARACTERISTICS

<u>Characteristic</u>	Media		
	Twisted Pair	Coaxial Cable	Fiber Cable
Weight	Low	Medium	Low
Complexity	Simple	Moderate	Complex
Cost	Low	Medium	High
Capacity	Low	Medium	High
Interference/RFI	High	Low	None
Splicing/ Reconnection	Simple	Moderate	Difficult

II. COMPUTER NETWORKING STANDARDS

A. INTRODUCTION

This chapter will discuss the major standards that are important to the study of local area networks. The ISO computer network model will be discussed since this model has gained wide acceptance and is applicable to computer networks in general. Next, the IEEE 802 local area network standards will be examined. The chapter will conclude with a brief discussion of the Department of Defense standards.

Although all LAN products available in the market today do not necessarily conform to these standards, they provide an excellent reference point from which to judge products. Also, these standards reflect the best thinking of respected experts in the field of computer networking, and a good understanding of them will enable a manager to make a more informed decision on what type of LAN to procure.

B. INTERNATIONAL STANDARDS ORGANIZATION (ISO) NETWORK MODEL

By the late 1970's, the need for the development of standards for linking computers and computer networks was evident. In 1977, the International Standards Organization (whose U.S. representation is provided by the American National Standards Institute (ANSI)) established a subcommittee to develop such an architecture. The resultant Open Systems Interconnection (OSI) reference model was adopted

in 1983. The model is a layered architecture, composed of seven layers each responsible for separate functions. A diagram of the basic model is shown in Figure 4.

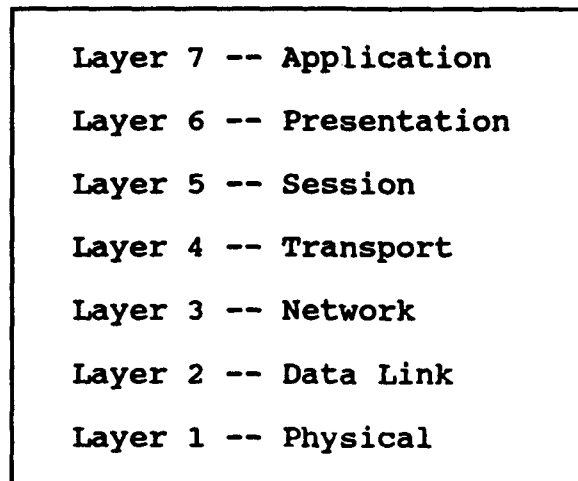


Figure 4. OSI Reference Model

The OSI model is important not only in local area networking, but in computer networking in general. To be sure, the ISO standards are not the only ones in existence. Table 3 displays general standards. Since the OSI reference model has gained wide acceptance, an understanding of the model will provide an excellent framework for local area networking topics to be discussed later. Therefore, the basic architecture and functions of each layer will be discussed.

TABLE 3
STANDARDS AND STANDARDS-MAKING ORGANIZATIONS
 [Ref. 3:p. 14]

Organization	Areas of Interest	Standards
International Organization for Standardization (ISO)	OSI model, layers 4-7	Transport, session
International Telegraph and Telephone Consultative Committee (CCITT)	Communications networks, telematics	X.25, X.75, X.21 ISDN
National Bureau of Standards (NBS)	Layers 2-7	Transport
Defense Communications Agency (DCA)	Layers 3-7	TCP, IP
Institute of Electrical and Electronic Engineers (IEEE)	Layers 1 and 2	IEEE 802
American National Standards Institute (ANSI)	Layers 1-7	FDDI
Electronics Industries Association (EIA)	Layer 1	RS-232-C, RS-449
Federal Telecommunications Standards Committee (FTSC)	Layers 1-3	Encryption
European Computer Manufacturers Association (ECMA)	Layers 1-7	Input to ISO

ISO chose to solve the problem of computer communications by using a structuring technique known as layering. Figure 5 shows a more detailed version of the ISO layered network model architecture. The dashed lines show virtual connections (the layers are not physically connected, but communicate as though they were). The only physical connection occurs at Layer 1, the Physical Layer. In the OSI reference model, each layer is responsible for its own functions (which will be described later), and for communicating only with those layers directly above and directly below.

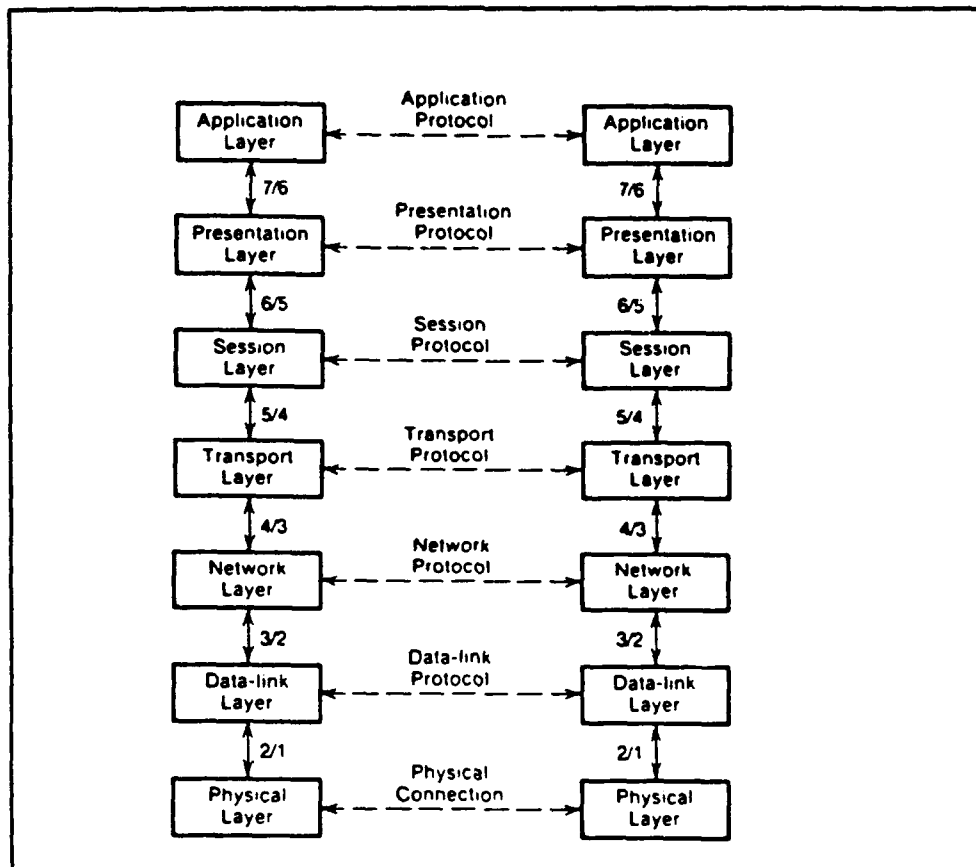


Figure 5. ISO Layered Network Model Architecture
[Ref. 15:p. 12].

The layered approach to LANs can best be described by the following principles:

- Each level should perform a well-defined function.
- The layers should comply with well-recognized standards if possible.
- Layer interfaces should be well defined and should be chosen to minimize information flow across the interfaces.
- The layer size should not be too large because that would make it unmanageable. Also, it should not be too small because that adds unnecessary complexity to the model. [Ref. 15:p. 12]

The layering technique of the OSI model breaks the complex problem of interconnection of computers into more manageable

segments. As explained in Table 4, the OSI model provides a framework for the development of standards at each layer.

TABLE 4
PURPOSE OF THE OSI MODEL
[Ref. 3:p. 390]

The purpose of this International Standard Reference Model of Open Systems Interconnection is to provide a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model.

The term Open Systems Interconnection (OSI) qualifies standards for the exchange of information among systems that are "open" to one another for this purpose by virtue of their mutual use of the applicable standards.

The fact that a system is open does not imply any particular systems implementation, technology or means of interconnection, but refers to the mutual recognition and support of the applicable standards.

It is also the purpose of this International Standard to identify areas for developing or improving standards, and to provide a common reference for maintaining consistency of all related standards. It is not the intent of this International Standard either to serve as an implementation specification, or to be a basis for appraising the conformance of actual implementations, or to provide a sufficient level of detail to define precisely the services and protocols of the interconnection architecture. Rather, this International Standard provides a conceptual and functional framework which allows international teams of experts to work productively and independently on the development of standards for each layer of the Reference Model of OSI.

Each of the OSI reference model layers will be discussed separately. Table 5 contains a brief explanation of the functions performed by each layer. Layer 1, the Physical Layer, will be discussed first since it is the foundation for the other layers.

1. Physical Layer (Layer 1).

This layer establishes the physical connection between computers, and is concerned with the flow of an unstructured bit stream over the chosen medium.

The physical layer has four important characteristics -- mechanical, electrical, functional, and procedural. Network

TABLE 5
THE OSI LAYERS
[Ref. 3:p.392]

1. Physical	Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the physical medium.
2. Data Link	Provides for the reliable transfer of information across the physical link; sends blocks of data (frames) with the necessary synchronization, error control, and flow control.
3. Network	Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining and terminating connections.
4. Transport	Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control
5. Session	Provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications.
6. Presentation	Provides independence to the application processes from differences in data representation (syntax).
7. Application	Provides access to the OSI environment for users and also provides distributed information services.

design issues which are addressed at this layer include type of cabling to use (i.e., copper wire or fiber optic cable, transmission waveform, maximum data rate, error checking of unstructured bit stream, and collision detection (if required). As the most fundamental layer, it is the most difficult and expensive to change. Therefore, decisions at the physical layer should take into account such factors as possible network expansion.

2. Data Link Layer (Layer 2)

This layer is responsible for structuring the bit stream passed to it from Layer 1 into frames, providing data flow control across the physical layer. Functions performed in addition to framing include:

- Frame sequencing (necessary for long messages with multiple frames).
- Addressing.
- Retransmission of damaged frames.
- Acknowledgement (ACK) or non-acknowledgement (NAK) of frames.
- Additional error checking.

Figure 6 shows some common LAN packet and frame formats. As can be seen, there are many ways of performing the same basic function. An explanation of frame contents is provided below:

- Preamble: a set bit pattern which allows all receivers to synchronize prior to transmission by the data-link layer.
- Synch: marks the beginning of a packet.
- Flag: used to mark beginning and/or end of frame.

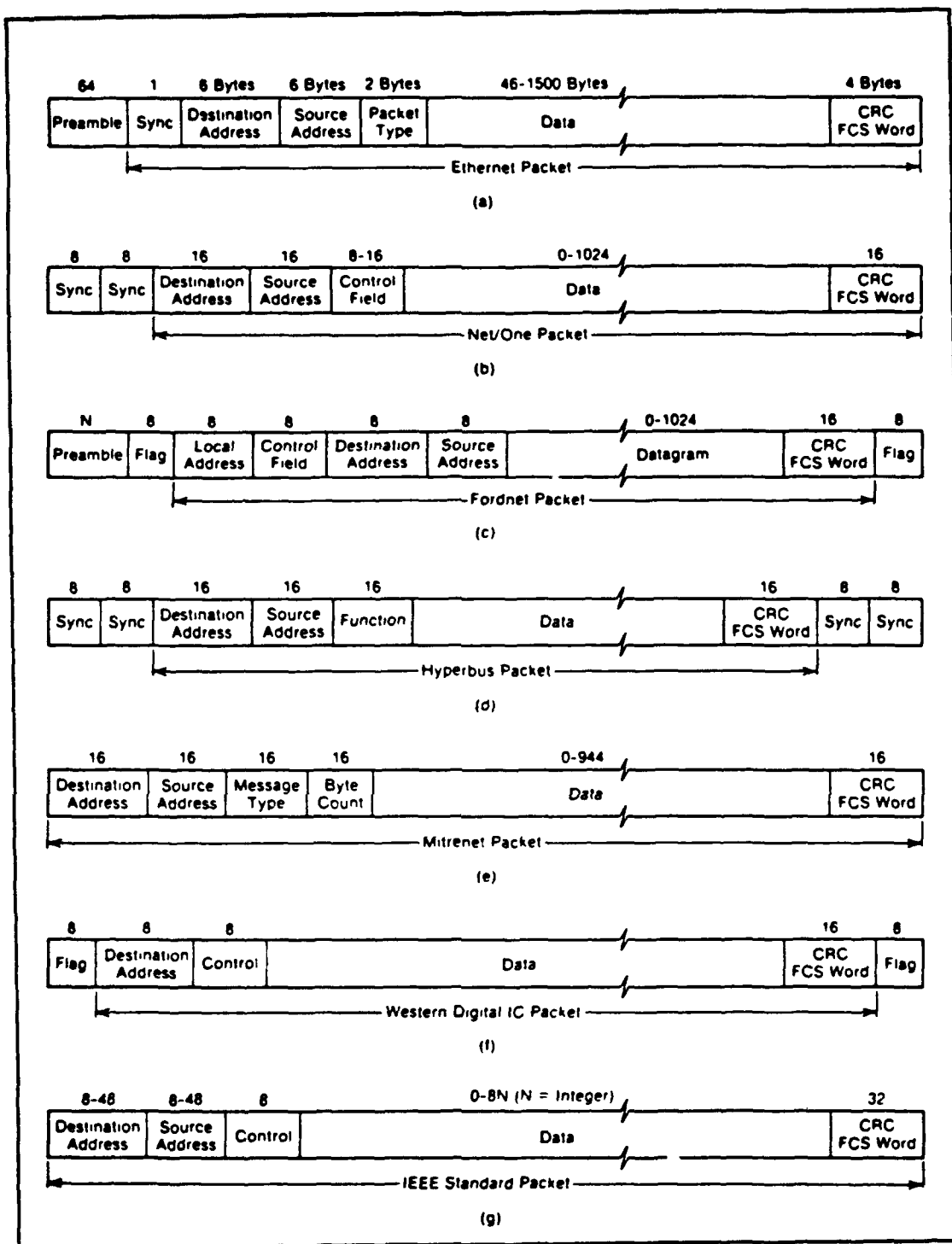


Figure 6. Common LAN Packet and Frame Format
[Ref. 15:p. 132]

- Control: can perform functions such as frame sequencing, ACK/NAK, polling, and others depending on the network.
- Address: the size of the source/destination address field can limit network size (for example, Net/One 16 bit address field allows for $2^{16} = 65,536$ addresses).
- CRC/FCS Word: error checking performed by Physical Layer (Layer 1).

As will be seen, frame contents will differ depending upon the type of network (i.e., Carrier Sense Multiple Access/Collision Detect Network vs. Token Passing Network), network size, or a variety of other factors.

3. Network Layer (Layer 3)

The basic service of the network layer is to provide for the transparent transfer of data between transport entities. It relieves the transport layer of the need to know anything about the underlying data transmission and switching technologies used to connect systems. The network service is responsible for establishing, maintaining, and terminating connections across the intervening communications facility.
[Ref. 3:p. 396]

The network layer also provides the functions of routing, traffic or flow control, accounting (for billing purposes), and maintaining system priorities. There are two basic types of network services -- virtual circuit or datagram. The virtual circuit is:

a packet switching service in which a connection (virtual circuit) is established between two stations at the start of transmission. All packets follow the same route, need not carry a complete address, and arrive in sequence.
[Ref. 3: p. 625]

Datagram is a method of transmitting messages in which segments of the message are allowed to be transmitted through

the transmission system without regard to the correct order, which will be determined by the receiving host. Of the two, virtual circuit is the more reliable and requires less intervention on the part of the upper layers. Table 6 shows a comparison of virtual circuits and datagrams. In the context of local area networks, the distinction between virtual circuits and datagrams is important when considering communication through a gateway to another network.

Routing on a network is accomplished by use of a fixed routing table, dynamic routing table, flooding (a broadcast technique, or directory routing. A fixed routing table is nonadaptive, whereas a dynamic routing table is adaptive and can take into account factors such as traffic flow. Flooding techniques are effective in ensuring message delivery but can saturate the network. The most common method used is directory routing, where the directory is set up by the operator using criteria such as shortest path, least delay, or light traffic volume. In local area networks, the network layer functions are virtually nonexistent since the broadcasting nature of LAN makes switching and/or routing unnecessary. Where this layer becomes more important is in internetworking (communications with other networks outside the LAN). This is where issues such as virtual circuits versus datagrams and routing techniques are more critical.

TABLE 6
COMPARISON OF VIRTUAL CIRCUITS AND DATAGRAMS
[Ref. 15:p. 162]

	<i>Virtual Circuit</i>	<i>Datagram</i>
Destination address	Only during initial start-up	Needed in every packet
Source address	Only needed at start-up	Not always needed
Error detection	Transparent to upper network layers	Done by the upper layers
Flow control	Provided by the network layer	Not provided by the network
Packet sequencing	Messages passed in order	No order required
Initial network setup	Required	Not possible

4. Transport Layer [Layer 4]

The function of the transport layer is to ensure that data units are delivered error-free, in sequence, and with no losses or duplications. [Ref. 3:p. 397] In terms of a local area network, transport facilities provide two functions:

1. Interprocessing of communications between local process and remote node processes.
 2. An additional error-checking capability.
- [Ref. 15:p. 214]

Figure 7 shows a typical LAN that requires a transport service. Using Node 1 as an example, terminal 1, terminal 2, and the printer can communicate without using the ring. However, to communicate with terminal 3, the transport layer would be used. Transport packets, if required, provide information similar to that provided in network packets. Transport packets are contained in the data segment of the network packet. Again referring to Figure 7, a packet from terminal 1 to terminal 4 would contain the destination node address in the datalink layer, and the destination terminal

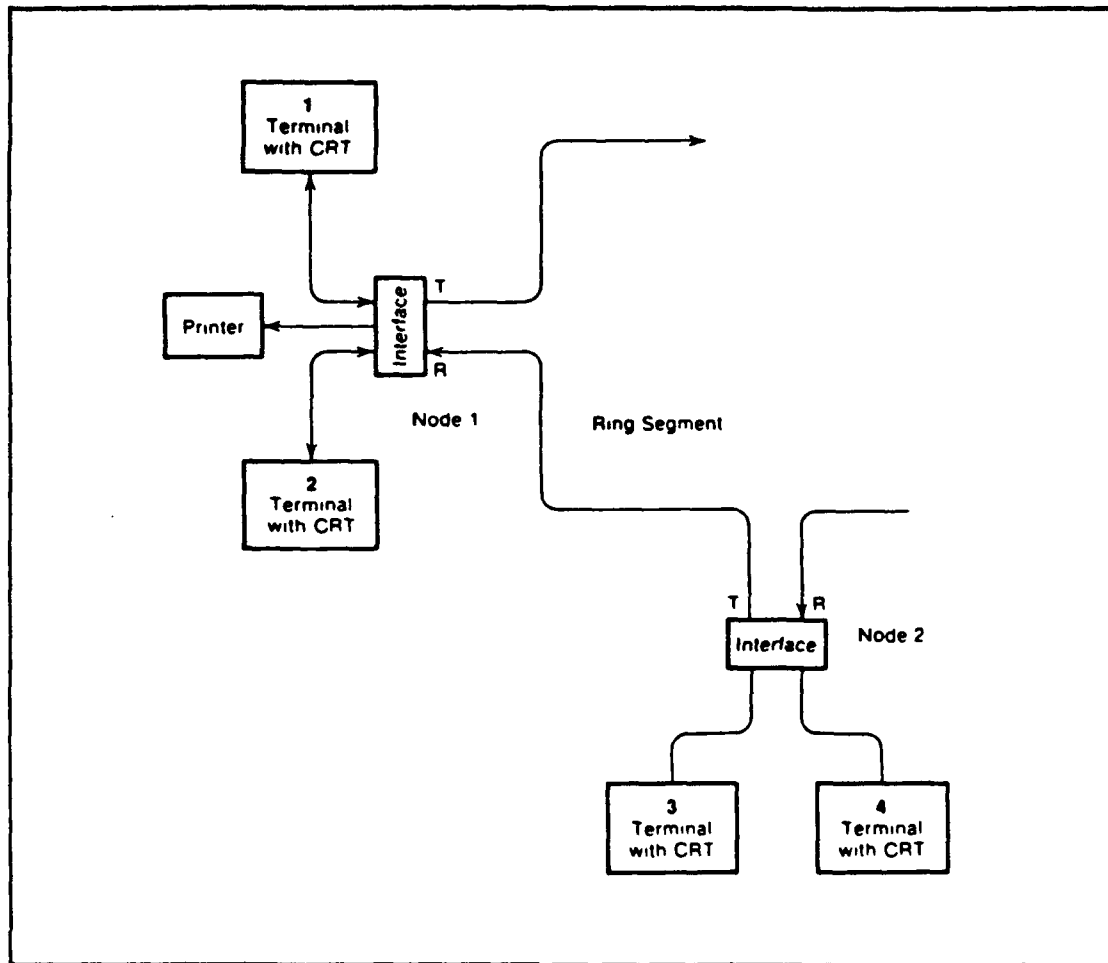


Figure 7. LAN Requiring Transport Service
[Ref. 15:p. 215]

address in the transport layer. Error correction and detection and packet sequencing also occur at the transport layer. [Ref. 15:p. 214-215]

5. Session Layer [Layer 5]

The session layer provides the interface between the hardware and software. While layers 1 through 4 are concerned with establishing and maintaining a physical connection, the session layer provides a user interface by enhancing the basic

connection service. Session layer features are grouped into the following categories:

- Session establishment and maintenance: When two users wish to establish a connection, a session is created and data is passed from the session layer to the transport layer for delivery.
- Dialogue management: Determines whether communication will be full duplex, half-duplex, or simplex (two way simultaneous, two-way alternate, or one way).
- Recovery: The session layer may contain the capability to recover lost data up to a certain point. [Ref. 3:pp. 522-525]

6. Presentation Layer [Layer 6]

As an interface between the application layer and the session layer, the presentation layer provides a common syntax for the exchange of data. In this way, files can be exchanged between hosts by negotiating an agreed-upon format. Other services which are a function of this layer are compression and encryption of data. This layer can also disguise one device as another (i.e., virtual terminal configuration) in order to facilitate the transfer of data.

7. Application Layer [Layer 7]

This is the layer most familiar to the end user. The application layer is responsible for making all other layers transparent to the operator of the equipment. [Ref. 15:p. 16] This layer does not carry out the application itself, but provides access to protocols such as E-Mail and file transfer.

C. IEEE 802 STANDARDS

Unlike the OSI model, which was developed for computer networks in general, the IEEE (Institute of Electrical and Electronics Engineers) 802 standards were developed specifically for LANs. The IEEE 802 standards have gained wide acceptance and have been adopted by ANSI as American national standards, NBS as government standards (non DOD), and ISO as international standards (ISO 8802). Accordingly, it is important to know what is included in these standards and how they differ from the OSI model. Figure 8 compares the IEEE 802 model to the OSI model. As can be seen, the IEEE 802 standards are primarily concerned with what were considered the network access protocols in the OSI model. In both models, the physical layer performs basically the same functions (with some exceptions). The medium access layer of the IEEE model provides a means for controlling access to the channel, for addressing the data frames, and for frame-checking sequences. The logical link control layer provides features similar to the data-link layer of the OSI model, and also some of the OSI network functions. A network layer is not identified in the IEEE 802 standard because the computers share a common channel and therefore routing and switching are not required. [Ref. 16:pp. 356-358]

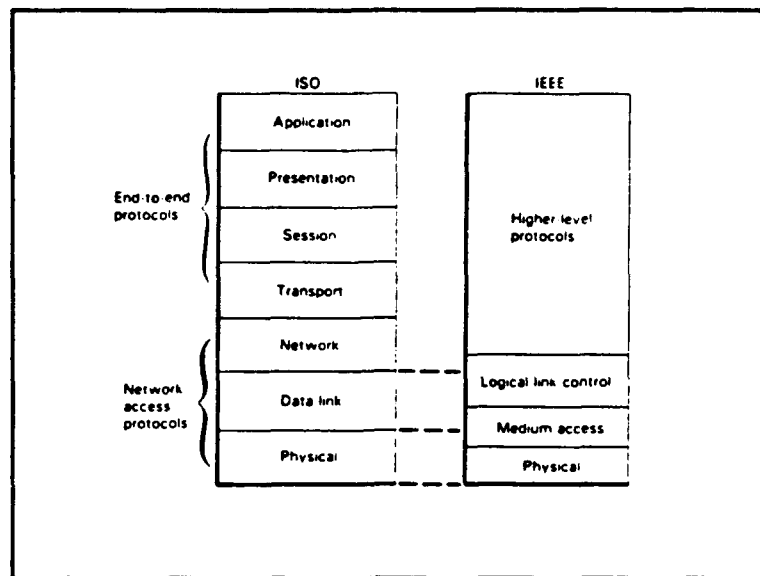


Figure 8. The ISO Model and the IEEE Local Area Network Reference Models Compared
[Ref. 16:p. 357]

The components of the IEEE 802 standard for local area networks are as follows:

- IEEE 802.1 Higher Layer Interface Standard
- IEEE 802.2 Logical Link Control Standard
- IEEE 802.3 CSMA/CD
- IEEE 802.4 Token Bus
- IEEE 802.5 Token Ring
- IEEE 802.6 Metropolitan Area Network

Figure 9 shows the hierarchy of the 802 standards and their relationship with the OSI model. As can be seen, the 802.1 and 802.2 layers are used by all other layers beneath them. The IEEE 802.1 standard describes the relationship between the components of the 802 standard, and defines the interface primitives. It need not be discussed in any greater detail, since applicable definitions will be covered in

discussion of the other layers. The IEEE 802.6 MAN standard is for a network that covers a much greater distance than a LAN (50 km in diameter), carries voice and video, and has speeds of several hundred Mbps. It is not a local area network, and will not be discussed any further. The remaining layers will be described below.

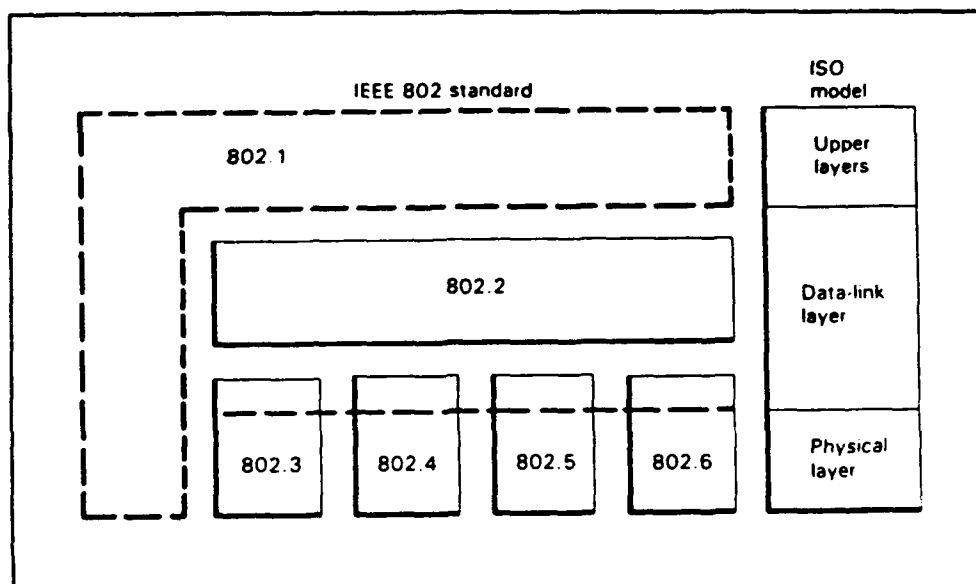


Figure 9. Component Parts of the IEEE 802 Standard and the ISO Reference Model
[Ref. 16:p. 356]

1. IEEE 802.2 Logical Link Control Standard (LLC)

The logical link control layer is concerned with establishing, maintaining, and terminating a logical link between devices on a LAN. The LLC provides three types of service to the upper layers of the LAN:

- Connectionless (Type 1): datagram-type service.
- Connection-oriented (Type 2): virtual circuit-type service.
- Acknowledged Connectionless (Type 3).

LLC services are made available to the upper layers by means of four types of service primitives: request, indication, response, and confirm. The meaning of these primitives is shown in Figure 10. The request primitive is used to pass a frame from the upper layers to the LLC for transmission. The indication primitive is used to pass a frame up from LLC upon reception. The meaning of response and confirm are as shown.

Primitive	Meaning
Request	An entity wants the service to do some work
Indication	An entity is to be informed about an event
Response	An entity wants to respond to an event
Confirm	An entity is to be informed about its request

Figure 10. Four Classes of Service Primitives
[Ref. 18:p. 24]

Unacknowledged connectionless service is the most simple. It is useful when upper layers of the OSI model are used to implement connections, or when it is not necessary to guarantee the delivery of data (i.e., real time applications involving a great deal of redundancy). Connection-mode service provides ordered delivery and error control, and relieves the upper layers of this responsibility. Acknowledged connectionless is simpler to implement than connection oriented, and is useful in a polling environment, or in a situation where the information is time critical

(i.e., alarm or control signal) and the sender needs to know it got through. [Ref. 17:pp. 56-57]

The IEEE 802 LLC primitives for connectionless, connection-oriented, and acknowledged connectionless service are shown in Figure 11. As can be seen, connectionless service is the simplest and has only two primitives. DL_UNITDATA.request is used to pass a frame down from the upper layers to LLC for transmission. DL_UNITDATA.indication is used to pass a frame from LLC to the upper layers upon reception.

As shown in Figure 11, the connection-oriented primitives are divided into five groups, as explained below:

- DL_CONNECT.: used to establish connections.
- DL_DATA: used to transfer data.
- DL_DISCONNECT.: used to release connections.
- DL_RESET: used to reset the connection after error detection. Sets all sequence numbers to zero.
- L_CONNECT_FLOWCONTROL: used to specify the amount of data that can be passed across the service access point (SAP). A serviceaccess point is a process or application having a separate address on the LAN.

Acknowledged connectionless service is actually two different services, DL_DATA_ACK and DL_REPLY. DL_DATA_ACK enables an LLC user to send data to another user and receive immediate confirmation of receipt of non-receipt. Only one data unit at a time may be outstanding. The DL_REPLY service is used to solicit data from a remote user, as in a

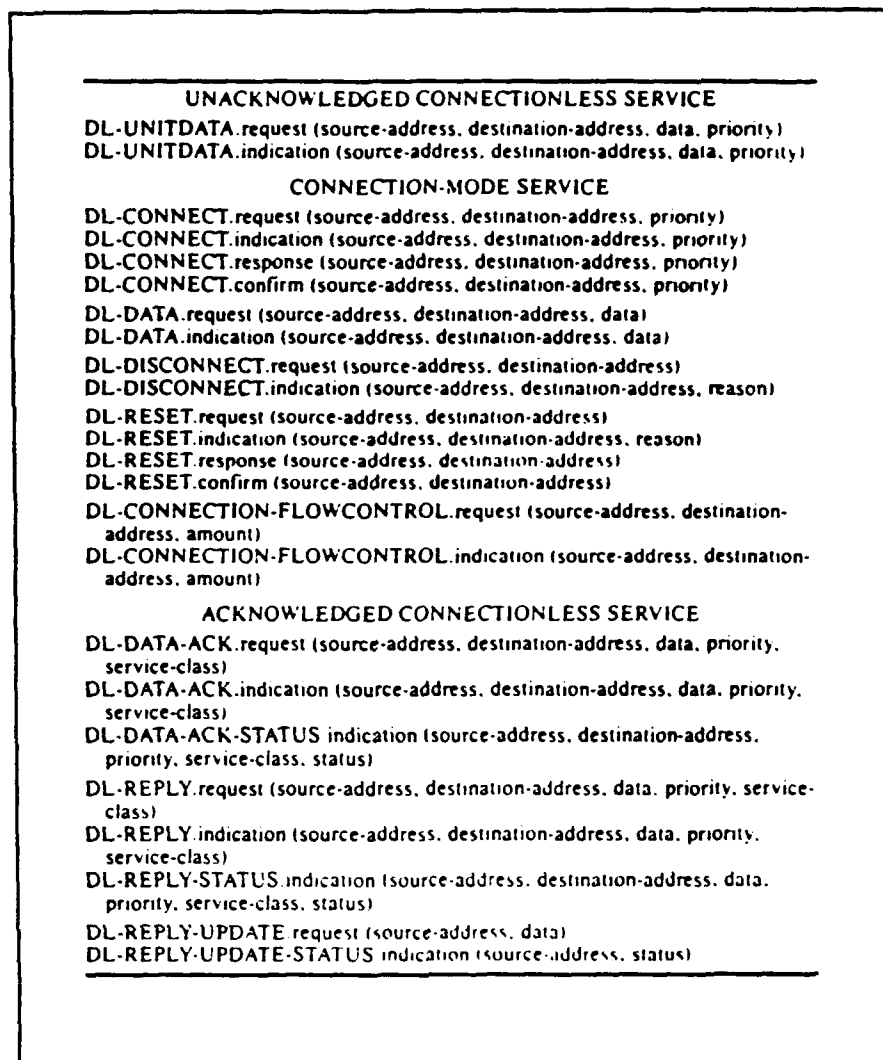


Figure 11. Logical Link Control Primitives
[Ref. 17:p. 54]

polling scheme, and may be used to transmit data at the same time. [Ref. 17:p. 64]

The primitives shown in Figure 11 define the interface between an LLC entity and its users. As stated earlier, the IEEE 802 LLC performs link control functions for all IEEE 802 medium access control protocols. The basic primitives for this interface are:

- MA_UNITDATA.request: To transmit LLC information transfer, supervisory, and unnumbered frames.
- MA_UNITDATA.indication: To deliver data transferred via an MA_UNITDATA.request.
- MA_UNITDATA_STATUS.indication: Passed from MAC to LLC to tell if the service provided for the MA_UNITDATA.request was successful.

The LLC frame format is shown in Figure 12. The contents of the four fields are explained below:

- DSAP address: Destination service access point address.
- SSAP address: Source service access point address.
- Control: Classifies the function and purpose of each frame into three different formats -- information transfer, supervisory, and unnumbered.
- Information: May or may not contain data depending upon the type of frame being transmitted.

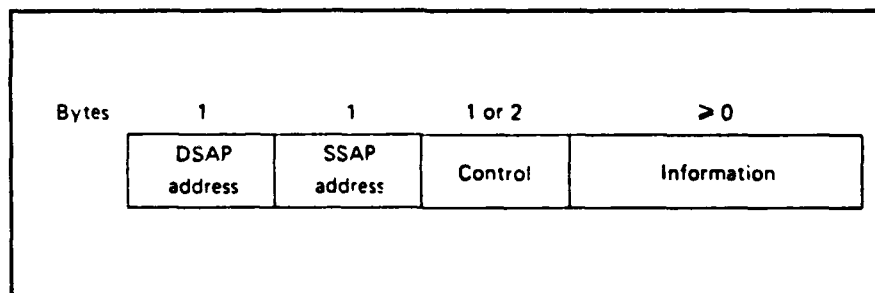


Figure 12: The IEEE 802 LLC frame format. This unit is carried in the data field of the MAC sublayer frame.
[Ref. 18:p. 265]

The complete list of LLC control frames is given in Figure 13. The "C" column indicates the code used for the frame type. The Format column (F) indicates the frame type (I = information transfer, S = supervisory, U = unnumbered). An "X" in the Command column (CMD) indicates the frame can be a command. An "X" in the Response (R) column indicates the

frame can be a response. Type 1 frames are used with connectionless, Type 2 with connection-oriented, and Type 3 with acknowledged connectionless transmission. [Ref. 18:p. 265]

It should be noted that the IEEE 802.2 LLC standard is not the only one which has been developed for logical link control over local networks. Two of the most prominent standards are ADCCP (Advanced Data Communication Control Procedures) developed by ANSI, and HDLC (High-level Data-link Control) developed by CCITT. These two standards differ only in some specialized options. IBM's SDLC is a minor modification to these standards. IEEE 802.2 is modeled after the HDLC balanced mode, with minor modification.

2. IEEE 802.3 CSMA/CD

The IEEE 802.3 standard is a medium access control for the bus topology which uses carrier sense multiple access with collision detection (CSMA/CD). This standard has its roots in the Aloha radio network discussed in Chapter One. The concept was further developed in the Ethernet system, which added carrier sensing while transmitting ("listen while talk"). Ethernet, developed by Xerox, formed the basis for the initial IEEE 802.3 standard. However, whereas Ethernet is generally limited to a 10 Mbps system using 50 ohm coaxial cable, the IEEE 802.3 standard has evolved to include different physical medium running at speeds of from 1 - 10 Mbps.

NAME	C	F	CMD	R	1	2	3
INFORMATION	I	I	X	X		X	
RECEIVE READY	RR	S	X	X		X	
RECEIVE NOT READY	RNR	S	X	X		X	
REJECT	REJ	S	X	X		X	
UNNUMBERED INFO	UI	U	X		X		
DISCONNECT	DISC	U	X			X	
SET ASYNCH BAL MODE EXTENDED	SABMF	U	X			X	
EXCHANGE INFO	XID	U	X	X	X		
TEST	TEST	U	X	X	X		
UNNUMBERED ACKNOWLEDGEMENT	UA	U		X		X	
DISCONNECTED MODE	DM	U		X		X	
FRAME REJECT	FRMR	U		X		X	
ACKNOW CONNECTION- LESS SVC SEQ 0	ACO	U	X	X			X
ACKNOW CONNECTION- LESS SVC SEQ 1	AC1	U	X	X			X

Figure 13: The IEEE 802 LLC frame types

The type of CSMA/CD which is used in the IEEE 802 standard is referred to as 1-persistent, and performs in the following manner:

1. If the medium is idle, transmit.
2. If the medium is busy, continue to wait until the channel is sensed idle, then transmit immediately.
3. If a collision is detected during transmission, immediately cease transmitting the frame, and transmit a brief jamming signal to assure that all stations know that there has been a collision.

4. After transmitting the jamming signal, wait a random amount of time, then attempt to transmit again.
[Ref. 19:p. 12-13]

In order for the collision detection aspect to be of value, the packets must be long enough to ensure collision detection prior to the end of transmission. If the packets were not that long, CSMA/CD would be no more efficient than CSMA without CD. [Ref. 18:p. 144]

Figure 14 shows the CSMA/CD frame structure. The individual fields are as follows:

1. Preamble. A 7-octet pattern used by the receiver to establish bit synchronization and then locate the first bit of the frame.
2. Start frame delimiter. Indicates the start of a frame.
3. Destination Address. Specifies the stations for which the frame is intended. It may be a unique physical address (one destination receiver), or a multicast-group address (all stations on the local network). The choice of a 16- or 48-bit address is an implementation decision, and must be the same for all stations on a particular local network.
4. Source address. Specifies the station that sent the frame. The source address size must equal the destination address size.
5. Length of data field. Specifies the station that sent the frame. The source address size must equal the destination address size.
6. Data. Field prepared at the LLC level.
7. Pad. A sequence of octets added to assure that the frame is long enough for proper CD operation. The minimum size is set as part of the physical layer specification.
8. Checksum (Frame check sequence). A 32-bit cyclic redundancy check value. Based on all fields, starting with destination address.
[Ref. 19:p. 12-13]

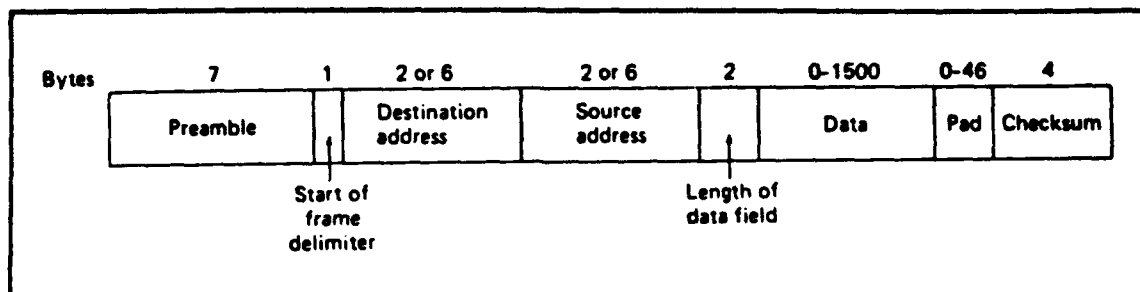


Figure 14. CSMA/CD frame format
[Ref. 17:p.144]

The physical layer specifications are as shown in Table 7. As can be seen, there are four different physical layer specifications, each of which provide a different level of service. The 10BASE5 specification is the original specification and is based on Ethernet. The 10BASE2 specification, also known as "Cheapernet", differs from 10BASE5 in that it employs a thinner cable. The cable is cheaper and easier to install, however: it supports fewer nodes at decreased node spacing due to the reduced capability of the thinner cable. The 1BASE5 specification provides an even cheaper alternative. Known as a "StarLan", it utilizes unshielded twisted pair and supports a data rate of only 1 Mbps. This specification employs a physical star, logical bus configuration. This means that although the LAN is arranged physically as a star, its logic is that of a bus in that a transmission from one station is received by all stations, and if more than one station transmits at a time, there will be a collision. The 10BROAD36 specification is the broadband version of CSMA/CD.

TABLE 7
IEEE 802.3 PHYSICAL LAYER ALTERNATIVES
[Ref. 17:p. 102]

Parameter	10BASE5	10BASE2	1BASE5	10BROAD36
Transmission medium	Coaxial cable (50 ohm)	Coaxial cable (50 ohm)	Unshielded twisted pair	Coaxial cable (75 ohm)
Signaling technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Broadband (DPSK)
Data rate (Mbps)	10	10	1	10
Maximum segment length (m)	500	185	500	1800
Network span (m)	2500	925	2500	3600
Nodes per segment	100	30	•	•
Node spacing (m)	2.5	0.5	•	•
Cable diameter (mm)	10	5	0.4-0.6	•
slotTime (bit times)	512	512	512	512
interFrameGap (μ s)	9.6	9.6	9.6	9.6
attemptLimit	16	16	16	16
backoffLimit	10	10	10	10
jamSize (bits)	32	32	32	32
maxFrameSize (octets)	1518	1518	1518	1518
minFrameSize (octets)	64	64	64	64

Recently, the 10BASET specification has been added to IEEE 802.3 standards. It is a high-speed (10Mbps) version of 1BASE5 which uses unshielded twisted-pair.

3. IEEE 802.4 TOKEN BUS

The token bus technique is more complex than CSMA/CD. As the name implies, IEEE 802.4 is also a specification for a bus network. However, the stations on the bus form a logical ring, and access to the medium is controlled by the use of a token. The station which has the token has control of the medium for up to a designated period of time and will pass control to its successor when it has no frames to send, it has sent all of its frames, or its time is up. With a token bus

network, the ordering of the logical ring does not need to be the same as the physical ordering of the devices on the bus.

Figure 15 shows the frame structure for token bus. The fields are as follow:

1. Preamble. A one or more byte pattern used by receivers to establish the synchronization and locate the first bit of the frame.
2. Start delimiter (SD). Indicates start of frame.
3. Frame control (FC). Indicates whether this is an LLC data frame. If not, bits in this field control operation of the token bus MAC protocol. An example is a token frame.
4. Destination address (DA). As with CSMA/CD.
5. Source address (SA). As with CSMA/CD.
6. Data unit. Field prepared by LLC, or used for MAC management signals.
7. Frame check sequence (FCS). As with CSMA/CD.
8. End Delimiter (ED). Indicates end of frame. [Ref. 19:p. 18]

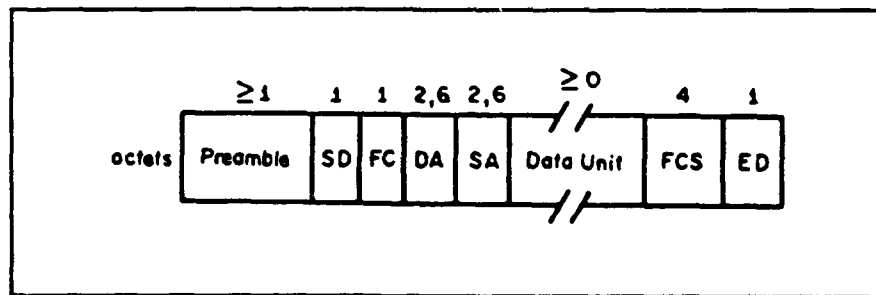


Figure 15: Token bus frame format
[Ref. 19:p. 18]

A token bus network requires considerable maintenance. The functions of ring initialization, additions to the ring, deletions from the ring, recovery, and priority must be

performed by one or more stations on the bus. [Ref. 17:p. 121]

Ring initialization occurs when there is a lack of bus activity for longer than the designated time out value. This condition can occur if the station holding the token fails, or when the network is being powered up. When this occurs, a claim-token frame is issued and stations will contend for the token. Once the contention is resolved, the ring is rebuilt. [Ref. 17:p. 126]

Additions to the ring are done by using response windows. Each node on the ring has a logical predecessor and a logical successor. Periodically, each node will issue a solicit-successor frame, which will give nodes with an address between itself and its logical successor an opportunity to enter the ring. If there is no response, the node will transfer the token to its logical successor as usual. If there is one response, the node will issue a set-successor frame and transmit the token to the requesting node, which will now be its logical successor. If there are multiple responses to the solicit successor frame, the conflict will be resolved by use of an address based contention scheme. [Ref. 19:p. 19]

Deletions from the ring are a little simpler. If a node wishes to remove itself from the ring, it will wait until it receives the token. Then, it will send a set-successor frame to its predecessor and tell it to send the token to its

successor. In the case of node failure, the node will not pick up the token when it is passed to it, and its predecessor will take the necessary action to establish a valid successor. [Ref. 19:p. 19]

Recovery, or fault management, covers a number of situations as shown in Table 8. First, if a node holding the token hears a frame indicating that another node has the token, it will revert to a listen mode and drop the token. The number of token holders should drop to either one or zero. The next three conditions would occur during token passing. Once a node passes the token to its successor, it will listen for one time slot to make sure its successor is active. The following sequence of events will occur:

1. If the successor node is active, the token issuer will hear a valid frame and revert to listener mode.
2. If the token issuer hears a garbled transmission, it waits four time slots. If it hears a valid frame, it assumes that its token got through. If it hears nothing further, it assumes its token was garbled and reissues the token.
3. If the issuer does not hear a valid frame, it reissues the token to the same successor one more time.
4. After two failures, the issuer assumes that its successor has failed and issues a who-follows frame, asking for the identity of the node that follows the failed node. The issuer should get back a set-successor frame from the second node down the line. If so, the issuer adjusts its linkage and issues a token (back to step 1).
5. If the issuing node gets no response to its who-follows frame, it tries again.
6. If the who-follows tactic fails, the node issues a solicit-successor-2 frame with its address as destination and source address (every node is invited

to respond). If this works, a two-node ring is established.

7. If the solicit-successor tactic fails, it assumes that some major fault has occurred; either all other stations have failed, all stations have left the logical ring, the medium has broken, or the station's own receiver has failed. At this point, if the station has any more data to send, it sends that data and tries passing the token again. If not, it drops the token, ceases transmission, and listens to the bus.
[Ref. 17:p. 126-128]

Priority access on a token bus can be accomplished using a class of service mechanism. Four classes of service are established. A station holding the token will transmit its data in descending priority order until its time slot has expired. In busy networks, this scheme is helpful in ensuring higher priority traffic gets through.

TABLE 8
TOKEN BUS ERROR HANDLING
[Ref. 19:p. 19]

<i>Condition</i>	<i>Action</i>
Multiple Tokens	Defer
Unaccepted Token	Retry
Failed Station	"Who Follows" Process
Failed Receiver	Drop Out of Ring
No Token	Initialize After Timeout

The physical layer specifications for the token bus are shown in Table 9. The phase continuous carrierband and phase coherent carrierband are both single channel broadband systems, which are less expensive than multichannel broadband but have much less capability. The least expensive option is

the phase continuous carrierband, which operates at one Mbps. The phase coherent carrierband option is more expensive, but has a higher data rate of either five or ten Mbps. The final option is a full broadband system, which can carry multiple channels, including video. It is the most expensive, and can support data rates of one, five, or ten Mbps. [Ref. 19:p. 23]

TABLE 9
IEEE 802.4 PHYSICAL MEDIUM ALTERNATIVES
[Ref. 17:p. 139]

Parameter	Phase Continuous Carrierband	Phase Coherent Carrierband		Broadband		
Data rate (Mbps)	1	5	10	1	5	10
Bandwidth (MHz)	N/A	N/A	N/A	1.5	6	12
Center frequency (MHz)	5	7.5	15	*	*	*
Modulation	Phase continuous FSK	Phase coherent FSK		Multilevel duobinary AM/PSK		
Topology	Omnidirectional bus	Omnidirectional bus		Directional bus (tree)		
Transmission Medium	75-ohm coaxial cable	75-ohm coaxial cable		75-ohm coaxial cable		
Scrambling	No	No		Yes		

* = depends on channel. N/A = not available

4. IEEE 802.5 TOKEN RING

Token ring is predicted to be the most popular ring access technique in the United States, and is the only method for ring access standardized by the IEEE 802 committee. In token ring networks, a control token is passed around the ring sequentially. The node with the token is allowed to transmit, with all other stations repeating each bit as it is received. The specification is a single token protocol, which means the transmitting station will not issue a new token until the busy

token returns. This scheme means that there should be only one token on the ring at a time.

Figure 17 shows the frame formats for token ring. The individual fields are explained as follows:

1. Starting delimiter (SD). A unique 8-bit pattern used to start each frame.
2. Access control (AC). Has the format 'PPPTMRRR', where PPP and RRR are 3-bit priority and reservation variables, M is the monitor bit, and T indicates whether this is a token or data frame. In the case of a token frame, the only additional field is ED.
3. Frame control (FC). Indicates whether this is an LLC data frame. If not, bits in this field control operation of the token ring MAC protocol.
4. Destination address (DA). As in CSMA/CD and token bus.
5. Source address (SA). As in CSMA/CD and token bus.
6. LLC. As in CSMA/CD and token bus.
7. FCS. As in CSMA/CD and token bus.
8. Ending delimiter (ED). Contains the error detection (E) bit and the intermediate frame (I) bit. The I bit is used to indicate that this is a frame other than the final one of a multiple frame transmission.
9. Frame status (FS). Contains the address recognized (A) and frame copied (C) bits.
[Ref. 19:p. 25-26]

A station wishing to transmit must wait for a free token. A free token will have a token bit of zero in the AC field. The station grabs the token by setting the token bit to one, and can transmit until it runs out of data or the

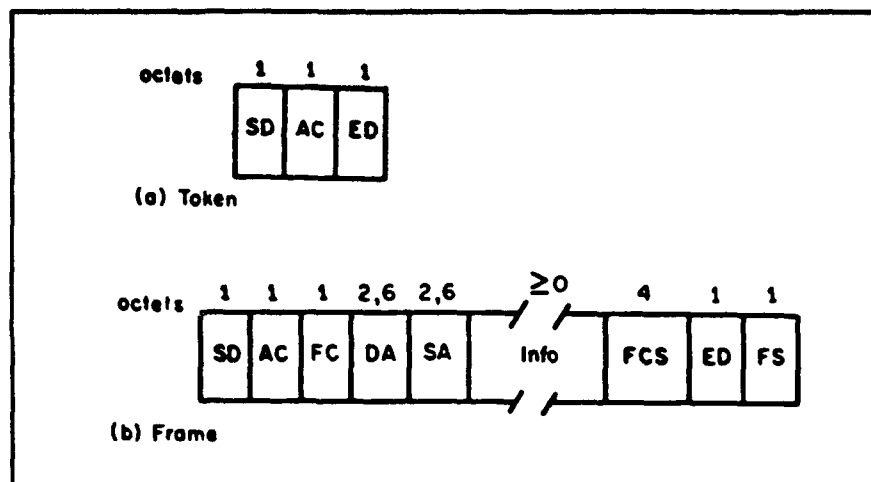


Figure 17: Token ring frame formats
[Ref. 19:p. 26]

token-holding timer expires. Once the busy token returns, the station will transmit a free token. [Ref. 19:p. 26]

Stations not transmitting will listen to the ring and do the following to passing frames:

- Perform error check: Set E bit to one if error detected.
- Perform address check: Set A bit to one if own address detected.
- Copy: If the message is addressed to the station, the station will copy and set C bit to one.

This will let the originating station know if the receiving station actually received a correct copy of the data.

The IEEE 802.5 specification also supports a multiple priority scheme for handling high precedence traffic. A station can reserve the next free token if the token being utilized has a lower priority level than the data the station needs to send. When the current token is returned to the originator, the currently transmitting station will issue a

free token at the higher priority. The token will then pass to the next station having equal or higher precedence data to send. When all high priority traffic is sent, the station that set the precedence is responsible for downgrading it to its former level.

One station on the ring is designated as active token monitor in order to detect and overcome error situations. Other stations are passive monitors. In the event of a failure of the active monitor, a contention-resolution algorithm will determine which station will take over.

The physical medium specified by the standard is shielded cable containing two balanced 150-ohm twisted pairs. Data rates of one to four Mbps are possible.

D. DEPARTMENT OF DEFENSE PROTOCOL STANDARDS

For purposes of discussion of local area networking standards, little or nothing need be said concerning Department of Defense (DOD) standards, because DoD standards are concerned with upper layers only and leave the specification of lower layers (network access layers) to other standard organizations. However, it is worthwhile to mention that there are DOD standards, which are used in military networks such as DDN. These standards evolved prior to the development of the OSI reference model and other standards. Figure 18 shows DOD protocol interfaces.

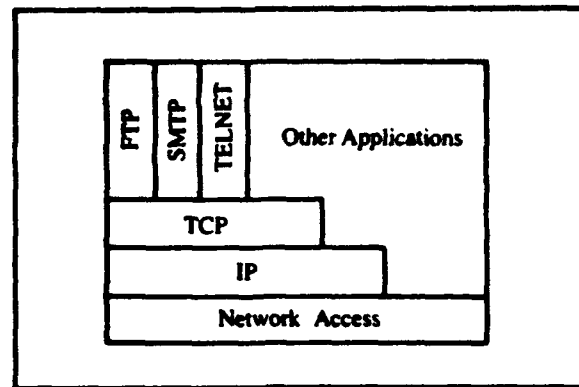


Figure 18. DOD protocol interfaces
[Ref. 20:p. 9]

In 1985, DOD made a commitment to transition from current DOD standards to the OSI architecture. This decision was based primarily on the wide commercial availability and superiority of OSI related products and the realization that DOD interests will be better served by transitioning to the international standards. [Ref. 20:p. 22-25]

III. LAN REQUIREMENT DETERMINATION

A. INTRODUCTION

Now that some of the technical issues involved in local area networking have been addressed, it is time to focus on factors which should be considered in determining if an organization would benefit from a LAN. It is important to bear in mind that the most vital factor is knowledge of the organization's requirements.

This chapter will discuss, on a basic level, the benefits that a LAN can provide. It is important to bear in mind that all LAN products do not provide the same level of service, but knowledge of basic capabilities can assist in determining requirements. This chapter will also address a method for determining requirements, and some alternatives to LANs which may be sufficient to satisfy organization's needs.

B. LAN SERVICES

Most local area networks will perform four basic functions--print service, mail service, file service, and remote access. Print service will permit personal computers on the network to print their output at any designated printer. This feature is extremely useful when a command has a high quality printer, such as a laser printer, which could be shared by network members. Mail service allows network members to send mail to others on the network. This feature

is useful in commands where a lot of interdepartmental liaison is required. The advantage of mail service over traditional face to face or telephone contact is that the other person does not have to be on the network in order to receive their mail. Using mail service, the supply officer can provide the training officer with a requisition status even though the training officer is attending a meeting elsewhere. This eliminates telephone tag and other inefficiencies involved in traditional means of communication. File services include file access, file transfer, and file archiving. These features are useful in cases where there is a lot of information that needs to be shared in the organization. For example, if the supply department had a computerized requisition status file, the training officer (who would have read-only access to the file) simply could have looked up the information himself. A good LAN will also support multiple users of applications programs, such as WordPerfect, Lotus 1-2-3, etc. Remote access is a feature which enables a LAN to connect to another network or a mainframe computer. This feature may be needed if there is a requirement to interact with a mainframe or computer network, or if there will be a need to do so in the future.

C. ORGANIZATIONAL REQUIREMENTS

Before a decision on local area networking can be made, it is essential to establish organizational requirements. A good requirements specification can simplify the decision making

process as well as facilitate the selection process if a decision to acquire a LAN is reached. In order to fully establish command requirements, the following are essential:

- Command support. The commanding officer must be fully supportive of the effort, and must make his/her position known to all personnel. This is important since all department heads may not be fully supportive of the effort without firm command guidance.
- Involve all departments. Although the original LAN initiative may have come from one department (i.e., admin, supply, etc.), the involvement of all departments is necessary to fully determine command requirements. Although this may seem like extra work, it will save a lot of time and effort later on.
- Provide clear direction. Each department should know exactly what is expected of them and who they can approach for assistance if needed.

The best way to determine requirements is to distribute a questionnaire, such as the one shown in Appendix A, and request the information by a specific date. The purpose of the questionnaire is to obtain answers to six main questions:

1. How many terminals and other simple digital machines must be supported?
 - What interfaces and protocols do they use?
 - Where are they and how much will they be used?
 - How often will they be moved and how quickly must they then be connected to the network?
2. What is the speed required of the network?
 - Is there any need to support computers and workstations that need fast file transfer?
 - What about speed of resource sharing?
3. How many host computers must be supported and with what interfaces?
4. Does the command need several incompatible networks in the same area?

5. Is there a need for voice/data integration?

6. What are the requirements for video communications?
[Ref. 8:p.36]

When all questionnaires from each department have been received, they should be consolidated and redistributed to all departments for possible update. This is especially recommended for larger commands where all departments may not be aware of the information processing capabilities of the other departments. Once the final data can be consolidated and tabulated, it should be possible to accurately establish if a valid requirement for a LAN exists.

The reason for distributing the questionnaire is to obtain a current snapshot of the way information is being processed within the command. If people are using peripherals located in other offices or departments, or there is a need to share information contained in databases, to exchange mail or access other networks, then acquisition of a LAN may be indicated. Note that a LAN should be purchased only if it provides the tools necessary to enable a command to function more efficiently. In an austere budget climate, few commands will be able to afford "nice to have" items. In order to be justified, the LAN should contribute substantially to effective mission performance.

D. LAN ALTERNATIVES

The primary alternative to local area networking would be maintaining the status quo. It may well be that after careful analysis of requirements that a LAN is not really needed.

Within the computer/communications communities, there are several debates that have been ongoing for a number of years over the relative merits of PBXs (Private Branch Exchanges), multi-user systems (dumb terminals connected to mini-computers), or Central Office (CO) LANs versus LANs. A brief discussion of each will follow:

- PBX versus LAN: The PBX has traditionally been used to support analog telephone communications. However, newer PBXs support digital communications, and can be used to network computers. The advantage of this approach is that separate wiring is not needed for the LAN, and there will be only one network to maintain. The disadvantage of this approach is that it is very expensive and the costs could rarely be justified for the transmission of data alone. However, commands in the process of updating their telecommunications systems and considering the procurement of a digital PBX may want to consider networking their computers in this manner. Bear in mind that the resulting network will probably be less robust than a LAN in terms of data rate and processing capabilities, since a PBX is little more than a switch.
- CO LAN versus LAN: CO LANs are offered by the telephone company, and commands currently using a CENTREX type of telephone system may want to consider this option. A CO LAN also uses existing telephone lines to connect computers. Under a CENTREX system, all calls are routed through the central office of the telephone company. Data is then either switched back to the premises (for intra-LAN processing), or sent outward (for inter-LAN communications). The advantage of this type of system is that existing phone lines are used and the only additional hardware required is one modem per terminal. This means that the cost of upgrading network features are borne by the telephone company. For commands reluctant to risk investing in an on-site LAN, this option may be worth pursuing.

However, as in the PBX alternative, CO LANs are less robust than most on-site LANs.

- Multi-user systems versus LANs: Multi-user systems feature a central computer (i.e., minicomputer) with dumb terminals connected to it. This type of system is ideal for transaction processing, and in situations involving many users, where cost per user is a key consideration. A dumb terminal cost less than a personal computer, and until capacity is reached, multi-user systems tend to be more cost effective than LANs. However, the cost of expansion of the network once the capacity of the minicomputer is exceeded is great. Also, since this thesis assumes that an activity already owns a number of IBM compatible personal computers, the multi-user system would not be a cost effective option.

If a requirements analysis concludes that the only need is for printer sharing within a relatively small area (i.e., admin office), there are printer servers which can perform this function at substantially less cost than for a LAN.

IV. STRATEGY FOR SELECTING A LOCAL AREA NETWORK

A. INTRODUCTION

Chapter Three discussed a method of determining if a LAN is needed by an organization. In this chapter, discussion will focus on differentiation between different types of LANs. First, a performance comparison of CSMA/CD, Token Bus, and Token Ring will be made. This will be followed by a study of the distinctions between the two most popular LAN topologies--Token Ring and Ethernet. Next, typical Ethernet components, both hardware and software, will be examined with a focus on the different levels of service which are available today. LAN products will be discussed with an emphasis on matching the product to requirements, and final discussion will focus on where to go for assistance if a command does not have the in-house personnel or expertise to accomplish a LAN acquisition.

B. PERFORMANCE COMPARISON BETWEEN CSMA/CD, TOKEN BUS, AND TOKEN RING

An important step in the process of deciding which LAN product to select is a determination of which type of LAN will best suit the needs of an organization. It is useful, then, to consider the performance characteristics of CSMA/CD, token bus, and token ring networks under different conditions. In 1985, such a study was undertaken by Bell Labs under the sponsorship of the IEEE 802 standards committee. The results are shown in Figures 19 through 22. [Ref. 3]

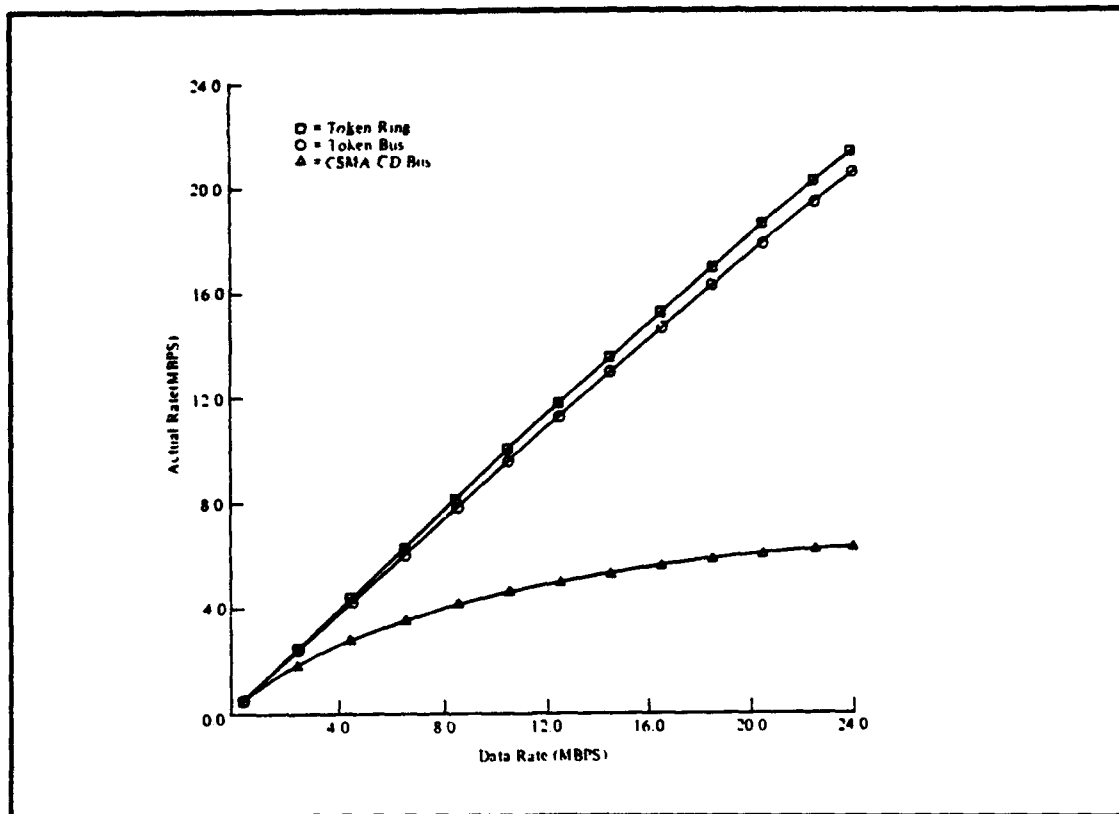


Figure 19. Maximum potential data rate for LAN protocols: 2000 bits per packet; 100 stations active out of 100 stations total. [Ref. 3:p. 364]

In Figure 19, there are 2000 bits per packet, and all 100 stations are active. In Figure 20, packet size is reduced to 500 bits per packet, with all 100 stations again active. Note the reduced effectiveness of CSMA/CD in comparison to Figure 19. This is because in order for the collision detection aspect to be of value, the packets must be long enough to ensure collision detection prior to the end of transmission. Clearly, at 500 bits per packet, its effectiveness was diminished. In both cases, the token networks were superior to the CSMA/CD network and token ring was superior to token bus.

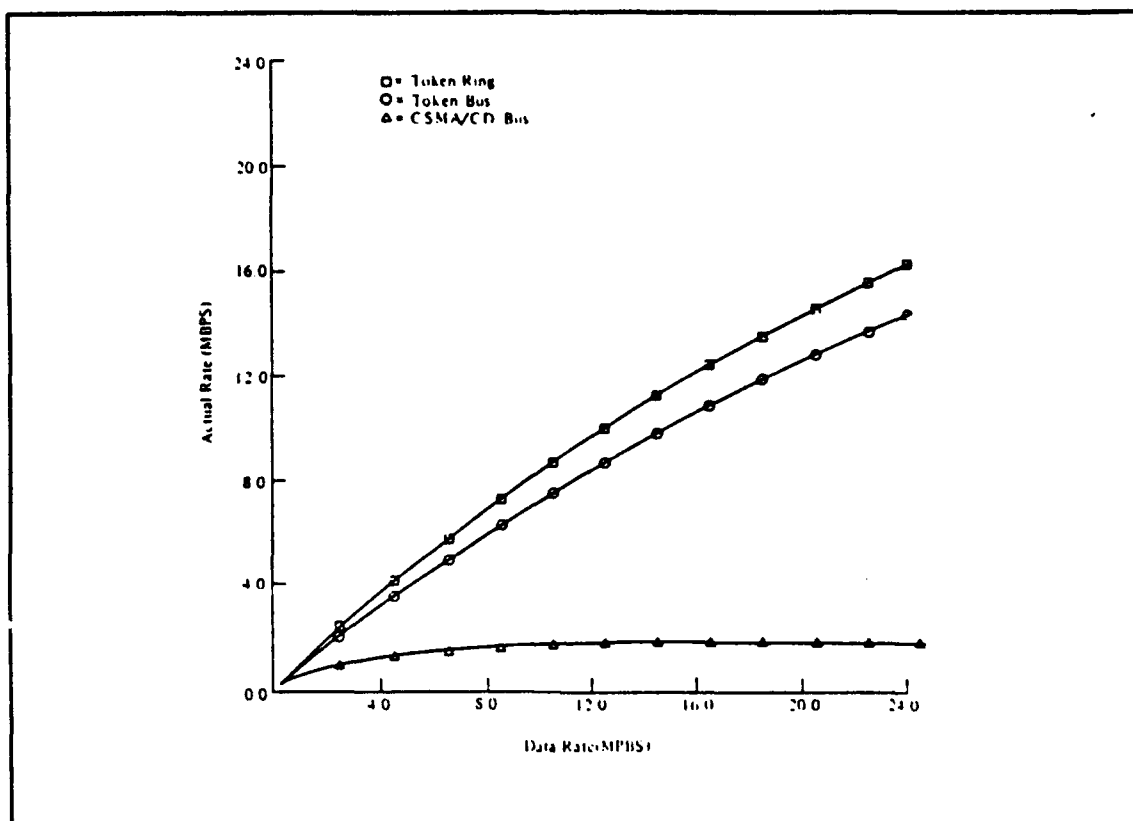


Figure 20. 500 bits per packet; 100 stations active out of 100 stations total. [Ref. 3:p. 365]

In Figures 21 and 22, only one station out of 100 is active. In Figure 21, a packet size of 2000 bits per packet was used, and the performance of CSMA/CD and Token Ring are nearly equal. Token Bus performance is substantially degraded, however, and this is due to a token processing delay greater than for token ring. [Ref. 3:p. 367] In Figure 22, packet size is reduced to 500 bits per packet, and the result is that token ring becomes clearly more efficient than CSMA/CD.

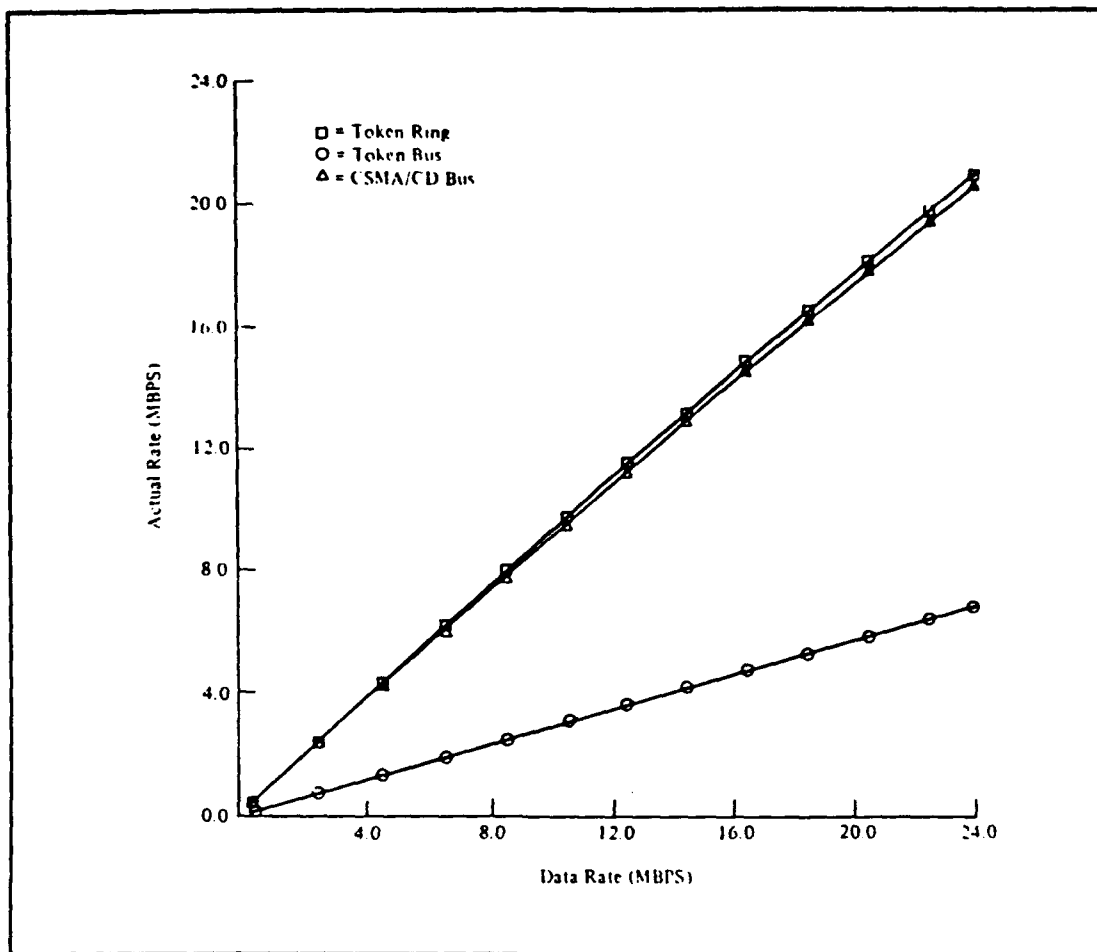


Figure 21. 2000 bits per packet; 1 station active out of 100 stations total.
[Ref. 3:p. 366]

In order to get a clear picture of what this data implies, it should be compared with specifications. For example, the IEEE 802.3 10BASE5 version of CSMA/CD uses a data rate of 10 Mbps. The IEEE 802.5 token ring uses data rates of up to four Mbps. When a comparison is made using those figures, it is clear that while under heavy traffic conditions the performance of a 4 Mbps token ring network is approximately equal (packet length of 2000 bits) or superior (packet length

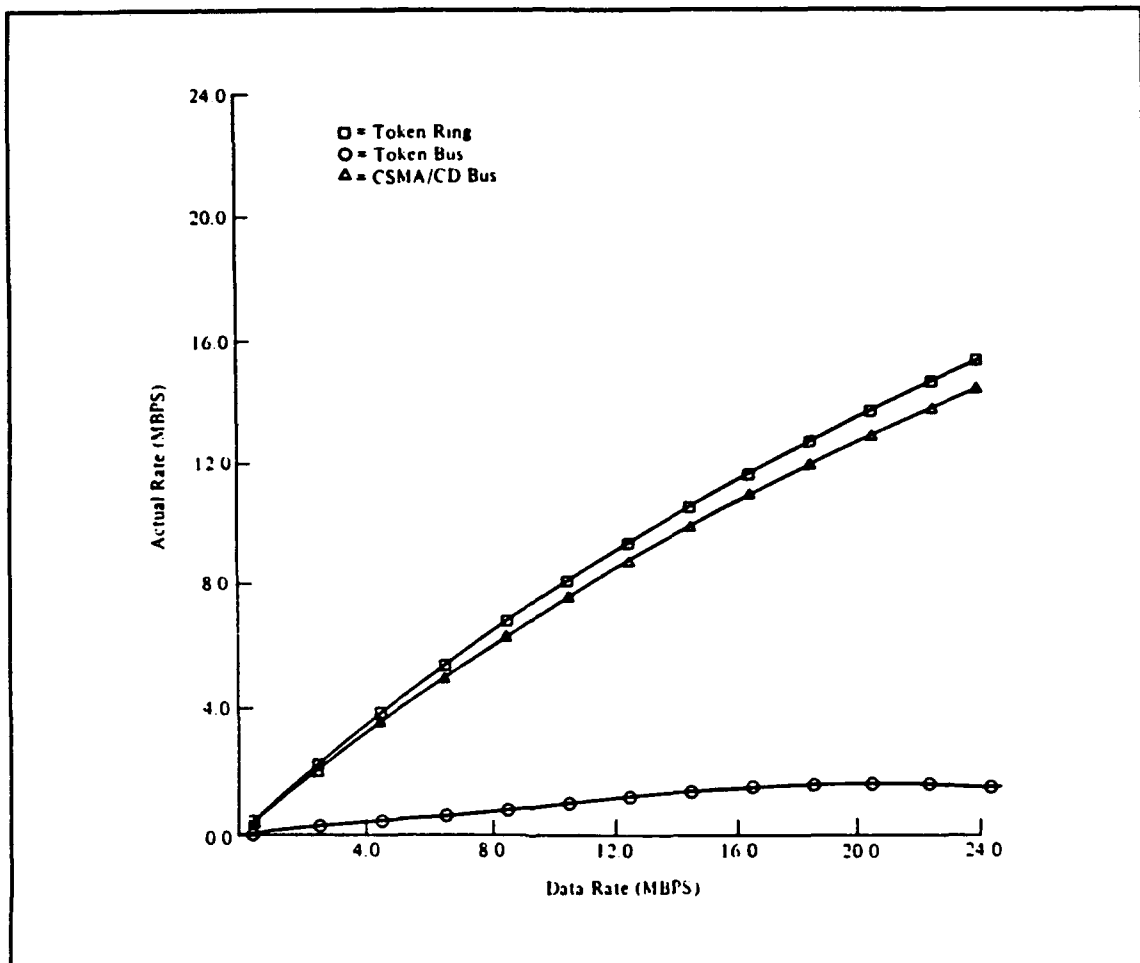


Figure 22. 500 bits per packet; 1 station active out of 100 stations total. [Ref. 3:p.367]

of 500 bits) to CSMA/CD. However, the situation is completely reversed under light conditions, with the 10 Mbps CSMA/CD network far superior to the 4 Mbps token ring. In short, "Ethernet is suited to applications that require less frequent network access but longer holding times while token ring is better suited to frequent access applications where access can be deterministically set to occur within some prescribed period of time". [Ref. 21:p. 27-28]

C. TOKEN RING VERSUS ETHERNET

A comparison of token ring and Ethernet is important for several reasons. Of the IEEE 802 standards, Ethernet and token ring have received the most vendor support and therefore most of the commercially available networks are either token ring or Ethernet. When a decision to procure a LAN is made, it will usually come down to a choice between these two. So it is important to know the relative advantages of each.

Ethernet has the advantage of being the oldest type of LAN. As such, it has the largest installed base. To date, it has received the most vendor support. In 1988, it was estimated that 57% of all LANs in the United States were based on Ethernet, 12% on token ring, and 21% on others (proprietary or other standards). [Ref. 22:p. 128] Additionally, Ethernet has been the LAN of choice for office environments, where network traffic is generally light.

Token ring, on the other hand, is more suited to a factory type of environment, where network traffic is heavy and there is a need to ensure equal or specified access to the network by each node. However, largely due to the impact of IBM and its Token Ring network, the use of token ring in the office environment has increased steadily. Additionally, IBM has announced a version of token ring that will run at 16 Mbps, which will make it even more attractive. It is predicted that "by 1991 or 1992 Ethernet and token ring will be about equal

in new sales volume as measured in total sales dollars".

[Ref. 21:p. 26]

From a practical standpoint, however, a token ring network is more expensive to implement than an Ethernet network due to increased hardware costs. That, in the end, may be the deciding factor. It is important to realize that both technologies will function effectively, and the differentiation lies primarily in the product performance of the LAN itself.

D. LAN COMPONENTS

A discussion of LAN selection strategy cannot be attempted without first defining typical LAN components. In addition to cabling and network topology, there are other features, both hardware and software, that are part of the LAN environment. Typical hardware which may be required for an Ethernet network is:

- Repeater: "A LAN component that regenerates digital signals, thus extending the length or interconnectivity of a communications medium". [Ref. 6:p. 54] A repeater is typically required when the length of cabling needed to connect a component (i.e., computer, peripheral) to the network exceeds IEEE maximum cable segment specifications.
- Transceiver: "A device that transmits/retrieves data to/from the devices on a local area network". [Ref. 6:p. 67] In some cases, the transceiver can be incorporated into the network interface card, which saves the cost of an external transceiver.
- Network Interface Unit (NIU): Used to connect network components (i.e., computer, peripheral) to the cable plant. There are three different types of network interface units -- asynchronous NIUs are used to connect devices such as dumb terminals and remote printers to the network, workstation NIUs provide connectivity for the

personal computer, and host NIUs are used to support minicomputer or mainframe communications.

- Server: "A specialized computer that provides a particular service, such as file or print service, to a network; increasingly, it comprises both the hardware and software which manage a network operation". [Ref. 6:p. 58]

The software which runs the network is referred to as the network operating system. The network operating system is the heart of the LAN, and it is what differentiates LAN products. Some of the major differences will be discussed below.

1. LAN Servers

LAN servers are either disk servers or file servers, and they perform their functions in either a centralized or distributed fashion. A disk server is available to all network members, and is usually partitioned to provide network users with a private storage area. Some disk servers provide for public storage areas which can be accessed by all workstations, but access to a particular file may be limited to one workstation at a time. File servers are more robust. Although the hardware is the same as a disk server, the file server provides greater software control over the hard disk drive. A dedicated server is a computer that handles only server functions, and all cables, connections, and data flows to it. A distributed server has the personal computers in the network performing server functions, which means that some of the personal computer memory is lost to the user in order to provide for the server. Table 10 shows the comparative

advantages and disadvantages of centralized versus distributed servers. In most cases, a centralized server is preferred. [Ref. 23:p. 71-72]

2. Network Control

Network control refers to the largest possible unit of a network that can be configured with respect to network resources. There are three levels of control -- workstation, server, and network. The minimum level of control is workstation control, where all the control possible under the network operating system is vested solely in the workstations. Information regarding user names, rights, files, pathways, and security can be placed only within each workstation, and can generally be changed by any user who logs onto the workstation. System configuration changes must be made at each of the effected workstations. Server control is a higher level of control where servers on the network store information regarding user names, rights, pathways, and security. In a single server network, network administrators can control network configuration from a single point. However, in networks with more than one server, a change in configuration will require changes at each server. Overall network control is the highest level of control, where the software recognizes the network as a whole, and the network can be administered from a single point regardless of the number of workstations or servers. [Ref. 24:p. 135-136]

TABLE 10. CENTRALIZED VERSUS DISTRIBUTED SERVERS

	CENTRALIZED	DISTRIBUTED
ADVANTAGES		
	Faster than distributed servers.	Lower start up costs because dedicated server not needed.
	Physical security easier to maintain.	Cost effective for small LANs which will not be expanded.
	File backup easier.	Loss of one workstation will not bring entire network down.
DISADVANTAGES		
	Cost	Loss of memory space for workstation functions.
	LAN inoperative if server goes down.	Server performance reduced by lack of memory resources.
		Server resources (such as files) not available unless workstation powered up.
		Physical security more difficult.
		Backups more difficult.
		Additional costs to provide required functionality may drive costs to that of dedicated server.

3. Pathways versus Names

The pathways versus names distinction refers to the way in which the network identifies objects such as users, files, directories, workstations, printers, and any other object

included in the LAN. Identification of objects is by pathway when access to a given object from any other object requires a statement of the path, routes, trees, or other structures the network must travel to find the object. Pathway schemes are acceptable in small, static network environments. Identification of an object is by name when access requires only that the user state the name of the object sought. This technique is superior to the pathways method. The most robust technique is hierarchical naming in which names consist of three parts -- local name, domain, and organization. Similar to the method for assigning telephone numbers, this method allows for easy administration and reconfiguration of computer networks. [Ref. 24:p. 137-138]

4. Integration of Services

This refers to the degree in which network services are incorporated into the network operating system. At times, a single vendor cannot provide all the services a user requires. A third party may provide a solution, however, usually additional hardware will be needed.

In addition to communications within the LAN itself, there may be a requirement to interface with other networks. This is accomplished through the use of bridges, routers, or gateways. Bridges are used for communication between LANs that use identical protocols for the physical and data link layers. Bridges operate at Layer 2 of the OSI model. Routers are used to connect dissimilar networks, and operate at Layer

3 of the OSI model. As such, routers are more complex than bridges but provide greater functionality. Gateways connect different network architectures by performing a conversion at Layer 7 of the OSI model. The gateway uses all layers of the OSI model plus all layers of the proprietary protocol, and is used, for example, to connect a local area network to a centralized mainframe.

E. LAN PRODUCTS

There are a multitude of LANs available today, which tends to complicate the selection process. However, a few common sense guidelines can make the process easier. First and foremost, stick with established vendors. Their products have gained credibility in the marketplace, are well-known (both good points and bad), and are generally well supported. Table 11 contains a comparison of three major Ethernet LAN products and the services they provide. This is not an endorsement of their products, but an illustration of some of the available services. It is important to remember that the LAN market is not static, and vendors are constantly upgrading their products to meet user demand.

TABLE 11. LAN PRODUCT COMPARISON
[Ref. 25: p.21]

Overview Network Operating System Design	Banyan VINES 3.0	Novell NetWare 286 v 2.1	3COM 3+Share v 1.3
Scheduled Tape Backup	INT/VEND	SA/VEND	INT/VEND
Electronic Mail	INT/VEND	SA/VEND	INT/VEND
Server to Server Communications	INT/VEND	SA/VEND	N/A (1)
Asynchronous Communications	INT/VEND	SA/VEND	SA/VEND
Host Communications	INT/VEND	SA/VEND	SA/VEND
TCP/IP Services	INT/VEND	SA/3rd	SA/3rd
Network PC Printing (Net printers via workstations)	INT/VEND	SA/3rd	N/A (2)
3rd Party Integration Possible? (Are facilities provided to allow 3rd party vendors to hook directly into NOS?)	*	*	*

Notes: (1) 3COM uses only bridges to link networks.
(2) 3COM has no (known) 3rd party solution for this.

Legend: * = Yes
INT = Part of NOS
SA = Stand-alone (requires separate PC)
VEND = Vendor provided (at least one) solution
3RD = 3rd party vendor provided (only) solution

Some other areas to consider are:

- Make sure the LAN can support the applications (data base programs, etc.) you plan to run.
 - Make sure that the network will support required connectivity to other networks.
 - Make sure the LAN supports security requirements such as restricted file access.
 - The network should be easy to maintain.
 - The network should be easy to expand.
 - A print spooler with a large buffer is needed for efficient printer sharing.
 - The network must support the personal computers you intend to connect.
- [Ref. 23:p. 76]

From a user perspective, the command must have a clear idea of their requirements and should evaluate vendors on their ability to meet them. Use of the questionnaire such as the one in Appendix A will give a good indication of LAN requirements. Further analysis of the data provide an estimate of the amount of bandwidth that will be required by evaluating the size of the applications currently used and the proposed amount of data transfer. Caution should be exercised in considering a cheaper, smaller bandwidth network. Most of these networks utilize unshielded twisted pair wire, which is inherently limited in network size and capacity. However, the new 10BASET standard has increased the data rate on unshielded twisted pair to 10 Mbps. While this makes this medium more attractive, it is still the most limited due to the

constraints discussed in Chapter One and should be used only in networks which intend to remain small.

It is important to determine where your computing assets are located and where additional equipment may be installed. Using the information obtained from the questionnaire, a floor plan should be developed showing the desired network configuration. Any physical restrictions should also be determined at this time. Restrictions may include conduit space for LAN wiring, or building codes requiring installation of wiring by certified electricians only. LAN cabling may be difficult to install, particularly if thick coaxial cable is used. The command needs to be aware of any factors which could potentially complicate the installation process. Also, just as in the installation of a new phone system, users need to be aware that the location of their computer equipment may have to change in order to accommodate cabling requirements.

Once a command has decided that they need a LAN and have determined their requirements, it is time to contact the base contracting officer who will assist in putting together the Request for Proposal (RFP). The RFP will contain precise requirements, and will be sent to vendors for bid. It is important to remember that normally the lowest bidder will get the contract, so it is important to make sure all requirements are explicitly stated. A good strategy to follow is to ask the contracting officer for any copies of RFP's he may have from commands which had similar requirements. If at all

possible, visit commands which have recently had LANs installed and find out if they are pleased with the product and service they have received from the vendor.

F. WHERE TO GO FOR HELP

Many commands simply do not have the personnel resources or in-house expertise to dedicate to a LAN acquisition project, particularly when it comes to preparing the exacting specifications of the RFP. Fortunately, assistance is available through the Naval Regional Data Automation Centers (NARDACs) and Naval Data Automation Facilities (NAVDAFs). On a reimbursable basis, the NARDAC will provide as much assistance as is needed, including requirements assessment, network design, and preparation of the RFP. Use of this service is highly encouraged, and a listing of NARDACs is contained in Appendix B.

V. CONCLUSION

The aim of this thesis has been to provide Navy shore based commands with sufficient information on local area networking to 1) decide if they need a LAN, 2) determine what their requirements are, and 3) select a LAN that satisfies their requirements. This has been accomplished by first providing an introduction into the technologies that made LANs possible, and describing the different LAN configurations (topologies). Medium access methods and transmission media were described in order to provide the background for more detailed discussion of computer networking and LAN standards in Chapter II. The importance of the OSI reference model to computer networking in general was emphasized, and the model was described in detail. The IEEE 802 LAN standards were explained, as well as their relationship to the OSI reference model and acceptance by the ISO standards organization. Chapter II laid the foundation for the remainder of the thesis by describing the LAN alternatives available through the different LAN standards. In Chapter III, emphasis shifts from the technical aspects of LANs to a practical description of the services a LAN can provide. A method for pinpointing organizational requirements was addressed, as were some of the more common LAN alternatives. Chapter Four presented a performance comparison between CSMA/CD, Token Bus, and Token Ring networks, later narrowing the focus to concentrate on differences between the two most popular networks -- Token

Ring and Ethernet. Components, both hardware and software, of an Ethernet LAN were discussed, emphasizing the different levels of service to be found in various products. The focus throughout the thesis was on determining current and future requirements of a command and selecting a product which provides the essential services. The following is a summary of the major conclusions:

- Navy shore-based commands considering acquisition of a LAN should first conduct a requirements analysis to determine if there is a valid need. The requirements analysis must have command support and include input from all departments. A good requirements analysis will provide a great deal of the information needed for LAN acquisition.
- Most Navy shore-based commands with a valid LAN requirement will find that an Ethernet network will best suit their needs. This is due to an Ethernet's lower cost (compared to token ring) and superior performance in an office automation environment.
- All commands will require file servers vice disk servers due to the unacceptable disk server limitations of inefficient disk partitioning and restricted file access.
- Most commands will need a centralized server. However, for small networks which will not be expanded, distributed servers may be acceptable.
- Workstation level control, where all the control possible under the network operating system is vested solely in the workstations, should be avoided since it is extremely difficult to manage. If a network is limited to one server, server control is sufficient. Network control is preferred for networks with more than one server. Server control for multi-server networks is possible, however, it is slightly more difficult to administer. This problem can be overcome by good procedures, so lack of network-wide control in a LAN product which is strong in other areas should not remove it from further consideration.

- A naming convention is preferred for larger networks or networks with frequent configuration changes. Pathway schemes are acceptable in small, static network environments. Choosing a network with a pathways convention means that the network will be less user friendly than a network using a naming convention. It also means that devices such as printers cannot be moved without changing every reference to the printer.
- Since a single LAN product may not meet all user needs, at times a third party solution will be required to provide a needed service. Users should be aware of the fact that this is not a part of the network operating system, and should determine its impact on the overall network environment.
- Many commands don't have the personnel or in-house expertise to dedicate to a LAN assessment. If this is the case, the Navy's LAN consultants at the NARDACs and NAVDAFs can provide assistance on a reimbursable basis.

Local area networking technology continues to improve. In the foreseeable future, fiber optic networks will run at 100 Mbps. LANs are becoming more user friendly, and much easier to manage. At the present, a LAN can provide a command with the services needed to operate more efficiently. The use of LANs will certainly increase, and hopefully this thesis has provided enough information to enable commands to make an intelligent choice concerning their LAN needs.

APPENDIX A

LOCAL AREA NETWORK REQUIREMENTS QUESTIONNAIRE

Instructions: Request this questionnaire be completed by _____ and returned to _____. If there are any questions, feel free to contact _____ at _____.

DEPARTMENT: _____

Does your department have any personal computers?

yes no

If yes, list

TYPE ROOM NUMBER

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Do you plan to relocate any personal computers?

yes no

If yes, for what reason?

List proposed relocations.

TYPE FROM TO

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

How quickly must they be reconnected?

Is relocation done on a regular basis?

yes no

If yes, what is frequency?

Is the number of personal computers adequate?

yes no

Do you currently utilize personal computers located outside your department?

yes no

If yes, list

TYPE ROOM NUMBER

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Does your department have any printers?

yes no

If yes, list

TYPE ROOM NUMBER

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Do you plan to relocate any printers?

yes no

If yes, for what reason?

List proposed relocations.

TYPE FROM TO

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

How quickly must they be reconnected?

Is relocation done on a regular basis?

If yes, what is frequency?

Is the number of printers adequate?

Do you currently utilize printers located outside your department?

If yes, list

Does your department have any other peripherals (i.e. plotters, scanners)?

If yes, list

Do you plan to relocate any peripherals?

If yes, for what reason?

List proposed relocations.

How quickly must they be reconnected?

Is relocation done on a regular basis?

If yes, what is frequency?

Is the number of peripherals adequate?

Do you currently utilize peripherals located outside your department?

If yes, list

Does your department currently access a host computer?

If yes, list.

yes	no
-----	----

yes	no
-----	----

yes	no
-----	----

TYPE	ROOM	NUMBER
_____	_____	_____
_____	_____	_____
_____	_____	_____

yes	no
-----	----

TYPE	ROOM	NUMBER
_____	_____	_____
_____	_____	_____
_____	_____	_____

yes	no
-----	----

TYPE	FROM	TO
_____	_____	_____
_____	_____	_____
_____	_____	_____

yes	no
-----	----

yes	no
-----	----

yes	no
-----	----

TYPE	ROOM	NUMBER
_____	_____	_____
_____	_____	_____
_____	_____	_____

yes	no
-----	----

TYPE	INTERFACE
_____	_____
_____	_____
_____	_____

List the applications programs
utilized by your department.

DATA BASE PROGRAM

List the data bases maintained and
applications programs they are run on.

Is the information in your database
utilized by other departments?

yes no

If yes, list.

DATA BASE DEPT

Do any of your personal computers
utilize modems?

yes no

If yes, list networks, mainframes, etc.
you interact with (i.e. DDN)

Do you presently prepare documents on
your personal computers for use by other
divisions?

yes no

If yes, list

In what form is your correspondence
presented to admin for typing?

computer disk
computer printout
handwritten
other _____

Would an intra-command electronic-mail
system be beneficial to your department?

yes no

Do you have a requirement for video
communications?

yes no

If yes, provide justification below.

APPENDIX B
NARDAC AND NAVDAF LOCATIONS

NARDAC Locations

Marketing Director
NARDAC Washington, DC
Washington Navy Yard
Washington, DC 20374
(202) 433-6435
AV 288-6435

Executive Officer
NARDAC Norfolk, VA
Norfolk, VA 23511
(804) 444-5428
AV 564-5428

Liaison-Planning Off
NARDAC Jacksonville, FL
Naval Air Station
Jacksonville, FL 32212
(904) 772-5276
AV 942-5276

Liaison-Planning Off
NARDAC New Orleans, LA
New Orleans, LA 70146
(504) 948-6425
AV 363-6425

Liaison-Planning Off
NARDAC San Diego, CA
NAS North Island
San Diego, CA 92135
(714) 437-5081
AV 951-5081

Liaison-Planning Off
NARDAC Pensacola, FL
Naval Air Station
Pensacola, FL 32508
(904) 452-2601
AV 922-3501

Liaison Planning Off
NARDAC San Francisco
Naval Air Station
Alameda, CA 94501
(415) 869-5203
AV 686-5203

NAVDAF Locations

Officer in Charge
NAVDAF Great lakes, IL
Bldg. 3200 Naval Training Center
Great Lakes, IL 60088
(312) 688-3456
AV 792-3456

Officer in Charge
NAVDAF Orlando, FL
BLDG. 2043, Naval Training Center
Orlando, FL 32813
(305) 646-4393
AV 791-4393

Officer in Charge
NAVDAF Corpus Christ, Tx
Bldg. 10, Naval Air Station
Corpus Christ, TX 78419
(512) 939-2681
AV 861-2681

Officer in Charge
NAVDAF Lamer, CA
Naval Air Station
Lamer, CA 93245
(209) 998-3514
AV 949-3514

Officer in Charge
NAVDAF Moffett Field, CA
Naval Air Station
Moffett Field, CA 94035
(415) 966-5556
AV 462-5556

Liaison-Planning Off
NAVDAF Pearl Harbor, HI
Box 140
Pearl Harbor, HI 96860
(909) 471-3888

Executive Officer
NAVDAF Newport, RI
Bldg. 11, Naval Education and
Training Center
Newport, RI 02840
(401) 841-2100
AV 948-2100

REFERENCES

1. Stallings, William, "Local Network Overview", Signal, v. 37, January 1983.
2. Halsall, Fred, Data Communications, Computer Networks and OSI, Second Edition, Addison-Wesley Publishing Company, 1988.
3. Stallings, William, Data and Computer Communications, Second Edition, Macmillan Publishing Company, 1988.
4. Liang, Ting-Peng, Ph.D., "Local Area Networks: Implementation of Considerations", Journal of Systems Management, v. 39, January 1988.
5. Lam, Simon S., Tutorial: Principles of Communication and Networking Protocols, IEEE Computer Society Press, 1984.
6. Network Glossary, Banyan Systems, Inc., June 1989.
7. Quinn, J.B., Mintzberg, H., James, R.M., The Strategy Process: Concepts, Contexts, and Cases, Prentice Hall, 1988.
8. Brillantine, Lance R., "Design and Selection Guide To Local Area Networks", Administrative Management, v. 46, October 1985.
9. National Bureau of Standards Special Publication 500-96, The Selection of Local Area Computer Networks, 1982.
10. Green, James Harry, The Dow-Jones Handbook of Telecommunications, Dow Jones-Irwin, 1986.
11. The Local Network Handbook, First Edition, McGraw Hill Publications Company, 1982.
12. Glass, Brett, "Fiber in Your Future", Infoworld, v.11, October 9, 1989.
13. Lefkon, Dick, "A LAN Primer", Byte, v. 12, July 87.
14. Southard, Robert K., "Fiber Optic Applications in Local Area Networking", Telecommunications, v.22, December 1988.
15. Baker, Donald G., Local-Area Networks with Fiber-Optic Applications, Prentice-Hall, 1986.
16. Hammond, J.L., and O'Reilly, P.J.P., Performance Analysis of Local Computer Networks, Addison-Wesley Publishing Company, 1986.

17. Stallings, William, Handbook of Computer-Communications Standards, Volume 2, Local Network Standards, Howard W. Sams and Company, 1987.
18. Tanenbaum, Andrew S., Computer Networks, Second Edition, Prentice Hall, 1988.
19. Pickholtz, Raymond L., editor, Local Area and Multiple Access Networks, Computer Science Press, Inc., 1986.
20. Stallings, William, Handbook of Computer-Communications Standards, Volume 3, Department of Defense (DOD) Protocol Standards, Macmillan Publishing Company, 1988.
21. Pyykkonen, Martin, "Local Area Network Industry Trends", Telecommunications, v. 22, October 1988.
22. Callahan, Paul and Bradley, Bob, "New Token Ring versus Ethernet: Counterpoint", Data Communications, v. 18, January 1989.
23. Lockwood, Russ, "Tying Computers Together: The Productivity Connection", Creative Computing, v.11, October 1985.
24. Bryce, James V., "Growing Pains", Byte, v.14, August 1989.
25. Local Area Network (LAN) Technology Overview (Draft), NARDAC San Francisco, undated.

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2. Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3. Chairman, Code AS Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
4. Curricular Officer, Code 32 Electronics and Communications Naval Postgraduate School Monterey, CA 93943-5000	1
5. Prof. Dan C. Boger (Code AS/Bo) Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
6. Prof. Myung W. Suh (Code AS/Su) Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
7. Chief of Naval Operations (OP-941) Navy Department Washington, DC 20350-2000	1
8. Chief of Naval Operations Director, Naval Communications/ Information Systems Division Washington, DC 20350-2000	2
9. LCDR P. A. O'Hara Box 135 NAVCAMSWESTPAC FPO San Francisco, CA 96630	2